2017-12

Follow the Silk Road: how Internet affordances influence and transform crime and law enforcement

Jerde, Ryan D.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FOLLOW THE SILK ROAD: HOW INTERNET AFFORDANCES INFLUENCE AND TRANSFORM CRIME AND LAW ENFORCEMENT

by

Ryan D. Jerde

December 2017

Thesis Co-Advisors: Rodrigo Nieto-Gomez
Lauren Wollman

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE FOLLOW THE SILK ROAD: HOW INTERNET AFFORDANCES INFLUENCE AND TRANSFORM CRIME AND LAW ENFORCEMENT			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ryan D. Jerde			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

A new category of crime has emerged in the border environment that is disrupting criminal typology. This new "hybrid" category intermixes physical and digital elements in ways not possible in the past. Internet technologies are facilitating this criminal evolution by affording perpetrators anonymity, efficiency, and distance. New criminal uses of the Internet have resulted in investigative challenges for law enforcement, especially concerning the illegal movement of people and goods.

This thesis mapped the evolution of hybrid crime using cases from the Silk Road and Silk Road 2.0, viewed through the lenses of stigmergy and affordance theory. While the research identifies challenges for law enforcement, it also uncovers methods for countering hybrid crime. I found that while criminals are opportunistic in perceiving new affordances to commit crime, law enforcement can be equally capable of countering them by removing technological barriers. Law enforcement can break down these barriers by changing mindsets, implementing smart enforcement, and relying on expertise from public-private partnerships.

14. SUBJECT TERMS affordance theory, media dependency theory, stigmergy, Silk Road, Operation Onymous, AlphaBay, Hansa, Operation Hyperion, BTC-e, hybrid crime, Internet technology, border, public/private partnership, narcotrafficking, drug trafficking, human trafficking, child exploitation, darknet marketplace, Tor, Bitcoin, cryptocurrency, smart enforcement, DARPA, Homeland Security Investigations, Federal Bureau of Investigation			**15. NUMBER OF PAGES** 135
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

FOLLOW THE SILK ROAD: HOW INTERNET AFFORDANCES INFLUENCE AND TRANSFORM CRIME AND LAW ENFORCEMENT

Ryan D. Jerde
Supervisory Special Agent, Homeland Security Investigations
B.A., Minnesota State University Moorhead, 1992

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2017**

Approved by: Rodrigo Nieto-Gomez
Co-Advisor

Lauren Wollman
Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A new category of crime has emerged in the border environment that is disrupting criminal typology. This new "hybrid" category intermixes physical and digital elements in ways not possible in the past. Internet technologies are facilitating this criminal evolution by affording perpetrators anonymity, efficiency, and distance. New criminal uses of the Internet have resulted in investigative challenges for law enforcement, especially concerning the illegal movement of people and goods.

This thesis mapped the evolution of hybrid crime using cases from the Silk Road and Silk Road 2.0, viewed through the lenses of stigmergy and affordance theory. While the research identifies challenges for law enforcement, it also uncovers methods for countering hybrid crime. I found that while criminals are opportunistic in perceiving new affordances to commit crime, law enforcement can be equally capable of countering them by removing technological barriers. Law enforcement can break down these barriers by changing mindsets, implementing smart enforcement, and relying on expertise from public-private partnerships.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CBP	U.S. Customs and Border Protection
CMU	Carnegie Mellon University
DARPA	Defense Advanced Research Projects Agency
DEA	Drug Enforcement Administration
DPR2	Dread Pirate Roberts 2
FBI	Federal Bureau of Investigation
FFRDC	federally funded research and development center
HSI	Homeland Security Investigations (ICE)
ICE	Immigration and Customs Enforcement
IRS	Internal Revenue Service
SEI	Software Engineering Institute (Carnegie Mellon University)

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY OF TERMS

Affordance Theory

A framework for analyzing the relationship between an object and all possible actions from that object. An affordance is the relationship between an object and the action. Some affordances are visible while others are only perceived.[1]

Bitcoin

A cryptocurrency that uses peer-to-peer transactions rather than a third party to process monetary transactions. Transactions are pseudo-anonymous, but recorded on a public ledger called a blockchain. Bitcoin was invented so transactions on the Internet could be "based on cryptographic proof instead of trust," which allows for decentralized payments outside of financial institutions.[2]

Bitcoin Tumbler

A third-party service used to mix transactions together from various sources as a way to make them more difficult to trace.[3] Tumblers make it so the blockchain cannot be used to trace transactions between buyers and vendors.[4]

BitTorrent

An open-source protocol that allows for the transfer of large amounts of data through the Internet by segmenting the data into smaller pieces. BitTorrent transmits data "by breaking it into small chunks, sending it through a peer-to-peer network, and reassembling it."[5]

Darknet Marketplace (or Cryptomarket)

A website hidden on the dark web that must be accessed through anonymizing software. Darknet marketplaces are used to sell illegal items such as drugs and guns.

---

[1] Don Norman, *The Design of Everyday Things*, rev. edition (New York: Basic Books, 2013), 10–13.

[2] Craig K. Elwell, M. Maureen Murphy, and Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, CRS Report No. R43339 (Washington, DC: Congressional Research Service, 2015), 3.

[3] Ian Allison, "Bitcoin Tumbler: The Business of Covering Tracks in the World of Cryptocurrency Laundering," *International Business Times UK*, February 13, 2015, http://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480.

[4] United States v. Ross William Ulbricht, Sealed Complaint, 1:13-cb-06919-KBF (SD NY, October 2, 2013), 15.

[5] Jessi Hempel, "The Inside Story of BitTorrent's Bizarre Collapse," Wired, June 19, 2017, https://www.wired.com/2017/01/the-inside-story-of-bittorrents-bizarre-collapse/.

Dark Web

A segment of the deep web used by criminal actors and terrorists to intentionally conceal illegal or subversive activities.[6]

Deep Web

Everything on the Internet that is not indexed by traditional search engines and may be protected by special software or hidden behind password-protected accounts. The deep web is used for storage of large databases owned by the government, LexisNexis, and internal networks used by companies and academic institutions.[7]

Honeypot

A method of enticing someone on the Internet to a specific site or part of a site for purposes of collecting information about motives and tactics.[8]

Media Dependency Theory

A sociological theory that explains why people support social networks by proposing there exists "an internal link between media, audience and large social system."[9] The theory proposes that people and media have "a relationship in which the capacity of individuals to attain their goals is contingent upon the information resources of the media system.[10]

Moore's Law

An observation that has held true for the last fifty years that computing power will double every two years.[11]

Stigmergy

A concept meant to explain how agents, including human beings, achieve self-organization in decentralized group settings.[12]

---

[6] Marc Goodman, *Future Crimes: Everything is Connected, Everyone Is Vulnerable and What We Can Do about it*, Kindle edition (New York: Anchor Books, 2015), 200–202.

[7] Ibid.

[8] William D. Eggers, *Delivering on Digital: The Innovators and Technologies that Are Transforming Government*, Kindle edition (New York: Rosetta Books, 2016), loc. 3327.

[9] "Media Dependency Theory," Communication Theory, accessed November 18, 2017, http://communicationtheory.org/media-dependency-theory/.

[10] Hsin-Yi Huang, Po-Lin Chen, and Yu-Chen Kuo, "Understanding the Facilitators and Inhibitors of Individual's Social Network Site Usage," *Online Information Review* 41, no. 1, (2017): 85.

[11] Robert L. Goldstone, Andy Jones, and Michael E. Roberts, "Group Path Formation," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 36, no 3 (May 2006): 612.

[12] Remi Pannequin and Andre Thomas, "Another Interpretation of Stigmergy for Product-Driven Systems Architecture," *Journal of Intelligence Manufacturing* 23 (2012): 2589.

Sybil Attack

An attack used to subvert communication flows in a peer-to-peer network by manipulating the assumed identities of relays.[13]

Tor

Free software that operates on a distributed network meant to anonymize a user's IP address, location, websites visited, and server locations by bouncing communications through several levels of encryption keys using a random selection of nodes around the world.[14]

Traffic Confirmation Attack

A computer attack that is done by controlling or observing entry and exit relays on both ends of a circuit to compare traffic timing, volume, or other characteristics so a determination can be made that the relays are on the same circuit.[15]

World Wide Web (or Surface Web)

The part of the Internet that is indexed and accessible by traditional search engines.

---

13 John R. Douceur, "The Sybil Attack," Microsoft, accessed November 18, 2017, https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf.

14 "Tor: Overview," The Tor Project, accessed November 18, 2017, https://www.torproject.org/about/overview.html.en.

15 "Tor Security Advisory: 'Relay early' Traffic Confirmation Attack," *Tor Blog*, July 30, 2014, https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis studies the changing typology of border-related crime being driven by Internet technologies. Internet technologies are moving elements of crime, understood to be physical, to the digital realm. Drug trafficking, human trafficking, and sexual exploitation, and money laundering are some of the crimes being facilitated by Internet technologies. The evolution of crime is so dramatic that a new category, dubbed "hybrid" crime, has emerged and is creating challenges for law enforcement. The goal of this thesis is to identify the challenges of enforcing laws against the illegal movement of people and goods when that movement is facilitated by the Internet.

Criminal use of the dark web, Tor, Bitcoin, and Bitcoin tumbler did not come about in a vacuum. Three pressures made the criminal environment ripe for transformative change. First, strong border enforcement made criminals search for new techniques that could facilitate crime. Second, new Internet technologies became available that could facilitate evolving physical criminal elements into digital elements. Third, as explained by media dependency theory, the criminal public transferred acceptance of online forums and social communities used on the Surface Web to darknet marketplaces, making the new technologies easy to accept. The result was the creation of hybrid crime.

The incorporation of new technologies facilitating crime calls for unique methods of analysis. Affordance theory and the concept of stigmergy are two frameworks not typically used for the study of criminal justice, but that hold promise for analyzing hybrid crime. Affordance theory is a conceptual framework of analysis used predominantly for the study of design.[1] This theory looks to understand and analyze object-action relationships.[2] For design theory, the intended purpose is to design products that function as perceived and desired; for the study of criminal justice, affordance theory can analyze

[1] Don Norman, *The Design of Everyday Things*, rev. edition (New York: Basic Books, 2013), 11.

[2] Ibid.

technology (the object) to determine possible actions (the affordance).[3] This type of analysis can help investigators understand individual technologies, predict future criminal uses, and even recognize when a new category of crime emerges. Affordance theory is especially adaptive in dynamic environments like the world of crime and technology.

Stigmergy complements affordance theory by explaining how decentralized groups with causal relationships self-organize even when they have no direct communication.[4] Criminal justice and deviant behavior have a causal relationship: when one of them commits to an action, the other has a reaction. In particular, law enforcement and criminals are part of a stigmergic cycle in which enforcement of crime affects how criminals act and the type of criminal tactics employed influence law enforcement responses.[5] When criminals use new methods, like Internet technologies, law enforcement must adapt by searching for new investigative techniques. The stigmergic cycle of law enforcement and crime dictates that a hybrid crime was created to overcome difficulties in committing border-related crimes using traditional means, but the starting point of the cycle is difficult to determine. This thesis uses affordance theory and the concept of stigmergy as a framework to analyze the Silk Road and Silk Road 2.0 darknet marketplaces. Both marketplaces provide ample information about the challenges involved with enforcing laws against the illegal movement of people and goods when that movement is facilitated by the Internet.

The Silk Road investigation is the best-documented example of how a large-scale darknet marketplace was used to implement Internet affordances to create hybrid crime. Despite successfully identifying and arresting the operator, Ross William Ulbricht, and seizing the Silk Road website, there is no indication that law enforcement successfully overcame the criminal benefits brought about by Ulbricht's Internet affordances. The dark web, Tor, Bitcoin, and Bitcoin tumbler all performed as Ulbricht had perceived to maintain anonymity. Instead of overcoming affordances, law enforcement was able to use

[3] Norman, *The Design of Everyday Things*, 4–12.

[4] Remi Pannequin and Andre Thomas, "Another Interpretation of Stigmergy for Product-Driven Systems Architecture," *Journal of Intelligence Manufacturing* 23 (2012): 2589.

[5] Rodrigo Nieto-Gomez, "Stigmergy at the Edge: Adversarial Stigmergy in the War on Drugs," *Cognitive Systems Research* 38 (June 2016): 3–5.

traditional law enforcement and established cybercrime techniques to capitalize on the vulnerabilities created when Ulbricht converted a purely physical crime into a hybrid crime. Law enforcement successfully located digital shadows on the Surface Web that helped them identify Ulbricht.

In contrast, the Silk Road 2.0 investigation shows law enforcement's success using unconventional investigative methods to overcome anonymity afforded by Tor. The Silk Road 2.0 darknet criminal marketplace was created after the demise of the Silk Road. Two of the operators, Blake Benthall and Brian Farrell, took Ulbricht's place after he was arrested.[6] What is interesting for this study is that although Benthall and Farrell had a basis for believing in their Internet affordances, as Ulbricht did, law enforcement changed the game by overcoming the anonymity afforded by Tor. After investigating the Silk Road, law enforcement started perceiving certain Internet affordances differently and adapted to them. When dealing with hybrid crimes, they developed response techniques outside of traditional investigative methods. In essence, law enforcement found a way to alter previously understood object-action relationships among Tor, anonymity, and hybrid crime. By relying on non–law enforcement technological expertise from the Carnegie Mellon University's Software Engineering Institute, law enforcement was able to overcome Tor anonymity and identify Silk Road 2.0's operators.[7] The Software Engineering Institute de-anonymized Tor by executing Sybil and traffic confirmation attacks on the Tor network.[8] This unconventional investigative technique is an example of law enforcement's adaptability in response to hybrid crime.

Criminals are continuing to rely on Internet technologies to commit border-related crime. This trend shows that drug trafficking has been proliferated by Internet technologies, but other crimes such as human trafficking and sexual exploitation and

[6]United States v. Blake Benthall, Sealed Complaint, 1:14-mj-02427-UA (SD NY, October 29, 2014), 8; United States v Brian Richard Farrell, Complaint for Violation, 2:15-cr-00029-RAJ (WD WA, January 17, 2015), 7.

[7] United States v Brian Farrell, Order on Defendant's Motion to Compel, CR15-029RAJ (WD WA, February 23, 2016), 1–2.

[8] "Tor Security Advisory: 'Relay early' Traffic Confirmation Attack," *Tor Blog*, July 30, 2014, https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack.

money laundering are also being influenced. The recent AlphaBay and Hansa darknet marketplace criminal cases show how prolific Internet technologies are in the drug trafficking world.[9] Several investigations involving live streaming from the Philippines highlight how Internet technologies are advancing child exploitation crimes. The BTC-e money laundering investigation, in which cryptocurrencies became the new tool for laundering illicit monies, demonstrates unique new ways of committing crime.[10] These examples show a continuing upward trend in hybrid crime, or at a minimum, a trend of physical crime elements converting to digital.

This study identifies several challenges that law enforcement faces when enforcing against border-related crimes that are facilitated by Internet technologies. To overcome enforcement challenges, this thesis found it essential to first properly label crime to determine efficient and effective investigative techniques, and to facilitate adequate analysis. Along with proper labeling, unconventional analytical frameworks, such as affordance theory and stigmergy, will benefit the study of criminal justice and aid in analyzing hybrid crime. One of the most important recommendations is to change mindsets about technology and crime through training. Law enforcement needs technology training and investigative support from technology experts. Once training is accomplished, smart enforcement techniques can be employed that focus on hybrid crime vulnerabilities and non-traditional enforcement techniques that can overcome criminal affordances. Smart enforcement measures need to be implemented that adapt to the dynamic environment of hybrid crime. Investigative techniques need to be properly matched to criminal vulnerabilities for digital, rather than physical, elements. Some techniques more competently investigate physical objects, and others digital. A primary

[9] "AlphaBay, the Largest Online 'Dark Market' Shut Down," Department of Justice, July 20, 2017, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down; "Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation," Europol, July 20, 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[10] "Russian National and Bitcoin Exchange Charged In 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox," U.S. Department of Justice, July 26, 2017, https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

strategy of smart enforcement should include attacking the level of trust being given to darknet marketplaces as a way to achieve deterrence.

This study found that criminals and law enforcement perceive Internet affordances differently, but that difference has not resulted in a large technology deficiency. Criminals use Internet technologies innovatively, but law enforcement is equally adaptive in its responses. Traditional investigative techniques have been effective against hybrid crimes when used at the time a criminal is transitioning physical elements to digital platforms. Unconventional methods that attack Internet affordances require more technical expertise to achieve, but have a greater impact against criminals. Despite the successes of traditional and unconventional methods, neither has effectively achieved general deterrence.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I have received substantial support from many people while attending this rigorous master's program at the Center for Homeland Defense and Security (CHDS). That support has come directly from CHDS, Homeland Security Investigations, and my family. Without that support, I would not have been able to accomplish such a demanding eighteen-month endeavor.

I want to start by thanking my thesis advisors, Drs. Rodrigo Nieto-Gomez and Lauren Wollman. They were a remarkable team that provided great ideas and guidance. Rodrigo helped devise this project from his big-picture ideas about technology and border security. His knowledge in this topic area and unique way of viewing problems helped make my project relevant and progressive. Rodrigo is truly a futurist. What can I say about Lauren, other than she is the sledgehammer who kept my project advancing? Her intellect and ability to guide past research sticking points and structural problems is amazing. Lauren will always have a special place in my heart, especially as I think about how many times I rewrote my literature review for her. Thank you so much.

I also want to thank Noel Yucuis, Greta Marlatt, and Scott Martis. Noel was incredibly generous with the time she devoted to improving my writing. Her guidance truly made my thesis a better product. Greta helped with research questions, library issues, and citation problems. Plus, she provided me with so much moral support that it made the daunting task of writing a thesis easier. Scott is the glue that keeps this program running and the cohorts cohesive. That cohesiveness is what will advance homeland security as we rely on each other to overcome future challenges. This brings me to thank my classmates in cohorts 1603 and 1604. You are remarkably good people and valuable to this discipline. Thank you for becoming my friends.

In addition to CHDS, my employer, Homeland Security Investigations, has been extremely supportive while I undertook this endeavor. I appreciate being allowed the opportunity to improve myself and learn new skills to advance homeland security. I especially want to thank Assistant Director Clark Settles, Special Agent in Charge Alex

Khu, Special Agent in Charge Patrick Lechleitner, Deputy Special Agent in Charge Tracy Cormier, Assistant Special Agent in Charge John Condon, Assistant Special Agent in Charge Gerard O'Neill, retired Assistant Special Agent in Charge David Atwood, Special Agent Jared Der-Yeghiayan, and Special Agent Martin Conley.

This program has been especially difficult on my family because I had to devote so much time to the rigorous academic demands on top of my normal employment demands. I truly appreciate my family's patience and apologize for being disengaged for eighteen months. I want to thank my beautiful wife, Karla, and my amazing children, Alexis and Evan, for their patience. I love all of you so much. I also want to thank my parents, sister, and brother for being a sounding board when I needed to vent about the buildup of work. Finally, I want to give a special thanks to my father- and mother-in-law, Hector and Eleonor, for keeping my household running each time I traveled to an IR. Hector, you are truly an amazing man and I am fortunate to be a part of your family.

Last, but certainly not least, I want to thank my amazing editor, Aileen Brenner Houston.

I am very humbled and thankful to each and every one of you.

I. INTRODUCTION

> It was really hard explaining the Web before people just got used to it because they didn't even have words like click and jump and page.
>
> —Timothy Berners-Lee, Inventor of the Internet[1]

A. PROBLEM STATEMENT

Today, a child is being sexually victimized because someone used the dark web to produce, create the customer base for, and distribute child pornography.[2] That criminal content will cross multiple international borders both as printed and online material. Today, a young girl is being bought and sold into prostitution, and criminals are using hidden online forums to make a sex trafficking transaction. She may then be trafficked to another country where she will be exploited.[3] Today, money laundering schemes are being facilitated by the electronic transfer of money through traditional United States banking institutions, through online purchases of stored value cards, or through virtual currencies. Those stored value cards or cash converted from virtual currency can then cross through international borders in the wallets of money launderers and drug dealers. Today, illegal immigration is facilitated by real identities, stolen from the Internet, that are used to make counterfeit documents. Heroin is being ordered online from a foreign country and shipped in plain sight to a U.S. customer through the U.S. Postal Service.[4] Sensitive technology and intellectual property are being stolen and sold through Internet facilitation, and then smuggled out of the country.[5]

---

[1] "Tim Berners-Lee Quotes," AZ Quotes, accessed December 6, 2017, www.azquotes.com/author/8668-Tim_Berners_Lee?p=5.

[2] Marc Goodman, *Future Crimes: Everything is Connected, Everyone Is Vulnerable and What We Can Do about it*, Kindle edition (New York: Anchor Books, 2015), 260, 262–263.

[3] Ibid., 261.

[4] Ibid., 256.

[5] *Cyber War: Definitions, Deterrence, and Foreign Policy*, Hearing before the Committee on Foreign Affairs to the Committee on Foreign Affairs, 114 Cong., 1 sess. (September 30, 2015), 7.

These are examples of crimes that use "Internet affordances" to circumvent law enforcement techniques deployed around national borders to avoid detection. In design studies, an affordance is defined as "a relationship between the properties of an object and the capabilities of the agent that determine just how the object could possibly be used."[6] Strategic management studies discuss affordance combined with technology, wherein "the use depends not only on the material properties or on the intended design of the tool, but also on the context and the interpretations of actors who may use the technologies in creative, unpredictable ways."[7] Internet affordances have lessened the effectiveness of border security techniques, for which enforcement strategies do not plan for an Internet component.

Cyberattacks and cyber intrusions are obvious direct risks from the Internet, but less obvious risks are initiated by actors who use the Internet to facilitate crimes traditionally only committed in the physical world. The Internet has provided these actors with a new means of committing criminal activity that is hidden from the physical world and often more difficult to identify. When law enforcement efforts are aimed at border security in the physical world, a person or good can easily be examined or inspected to determine criminal activity; this is not possible for crimes that cross a digital border. The investigative tools for examining or inspecting people or goods are less effective or completely impossible when transnational crimes are facilitated by the Internet.

To expand on the previous examples: child pornography can be electronically sent in or out of the United States without any physical object crossing the border; money laundering schemes can be completely virtual and will remain so until electronic funds are converted into currency; stolen sensitive technology or intellectual property does not ever need to be converted outside of the virtual world if it involves electronic data, plans, or digital media. Even though these Internet-facilitated crimes do not cross a physical border, they cause the same amount of harm to the physical world. These crimes fit well within the overarching category of cybercrimes, but others do not.

---

[6] Don Norman, *The Design of Everyday Things*, rev. edition (New York: Basic Books, 2013), 11.

[7] Paula Jarzabkowski and Sarah Kaplan, "Strategy Tools-In-Use: A Framework for Understanding 'Technologies of Rationality' in Practice," *Strategic Management Journal* 36 (March 2014): 539.

Drug trafficking, sex trafficking and sexual exploitation, and smuggling of bulk cash or stored value cards have a hybrid nature that allows them to affect both physical and digital borders. Sex trafficking is frequently facilitated by the Internet, which is used to entice victims and house hidden forums that advertise and "sell" the product of sex. Human trafficking relies on Internet facilitation to locate potential clients and collect fees. Drug trafficking can rely on individual buyers who order and pay for drugs completely online without ever visiting a "dark corner" or interacting face-to-face with a drug dealer. Illegal transfers of money can occur when someone transfers money electronically or adds value to stored value cards on the Internet. This is one way to launder proceeds of crime. Although these crimes are afforded by digital technologies, they do not neatly fit the definition of cybercrimes because they still depend on a physical, trans-border aspect. Sex and human trafficking victims must physically cross the border for the crime to occur. Drug traffickers, even if filling orders online, must still physically ship drugs across the border into the United States, often using the U.S. Postal Service for the illegal transaction. Bulk cash and stored value cards can begin as Internet-facilitated electronic transfers that are then withdrawn as physical currency so cash and cards can be smuggled across the U.S. border to avoid banking laws.

The Department of Homeland Security has primary responsibility for enforcement of border-related crimes, but it has no policy to specifically address the intersection of border enforcement and the Internet on the transnational scale—the United States does not build border security strategies with Internet-enabled threats in mind. Law enforcement currently has limited tools to effectively combat transnational crimes with online components and is not advancing investigative techniques as quickly as criminal actors are advancing their use of technology. Because the United States' border enforcement is almost blind on the Internet, a technology gap is believed to be growing between criminal actors and law enforcement. This technology gap continues to grow wider as organizational and cultural constraints limit law enforcement's ability to adapt.

A physical wall will not affect the Internet-based elements of transnational crime involving the illegal movement of people and goods in and out of the United States, but removing barriers that keep law enforcement from understanding technology will. The

Internet creates affordances that facilitate innovative ways of committing old and new crimes.[8] Understanding how those affordances work is a critical component of this thesis. If successful, this research will facilitate a more effective border security strategy and law enforcement techniques that are better able to enforce laws aimed at the illegal movement of people and goods facilitated by the Internet.

B. RESEARCH QUESTION

This thesis answers the question: What are the challenges of enforcing laws against the illegal movement of people and goods when that movement is facilitated by the Internet?

C. LITERATURE REVIEW

Internet technologies, criminal typologies, and border enforcement are diverse and complicated subject areas. This literature review summarizes material relevant to applicable topics, including Internet trends, the criminal environment, theoretical frameworks, technology, and cases involving darknet markets. Because this study involves disruptive technologies, contemporary criminal cases, and future studies, it was difficult to locate material on some of the important sub-topics. As a result, the review covers non-academic articles and media reports, in addition to scholarly journal articles, published books, and court documents.

1. Internet Complexity Defined by Cybercrime and Intrusions

To recognize the differing Internet affordances available to criminals and law enforcement, it is first necessary to understand how the Internet is used to facilitate crimes. There is significantly more material that addresses the complexity of Internet-facilitated cybercrimes and intrusions than border-related crimes. Even though most material about complexity does not directly involve border-related crimes, Internet complexity involving any criminal activity is valuable to understanding others. This

[8] Daniel Robey, Chad Anderson, and Benoit Raymond, "Information Technology, Materiality, and Organizational Change: A Professional Odyssey," *Journal of the Association for Information Systems* 14, no. 7 (July 2013): 386–389.

section of the literature review shows how the Internet's complexity is reflected in the literature through pervasiveness of crime, lack of definitional consensus, and explanations of dark web disruptive technology.

Published books, government testimony, journal articles, and media reports were the primary sources reviewed to understand the complexity of cybercrimes and intrusions. A large amount of literature confirms the pervasiveness of cyberattacks and intrusions. The material consistently uses case studies to explain the severity of the problem and to associated costs. For example, Goodman explains that losses from the 2007 TJX hacker attack resulted in the theft of ninety-four million customer credit card details, with a true cost of over $1 billion.[9] He also notes that an estimated $400 billion is lost globally each year to cybercrime.[10] Riley, Elgin, Lawrence, and Matlack analyze a 2013 malware attack against Target department stores that resulted in 70 million stolen credit card and debit card account credentials, costing in excess of $1 billion.[11] Elkind discusses the 2014 Sony Pictures Entertainment cyberattack, during which sensitive data was stolen and half of Sony's network erased.[12] This literature demonstrates a pervasive cyberattack pattern and shows that criminal actors have Internet affordances that law enforcement do not, and that law enforcement has not been capable of deterring criminal behavior away from the Internet.

The complexity is especially apparent when one attempts to define the actions that make up cybercrime, cyberterrorism, and cyberwar. Holt discusses the problems of defining cybercrime and cyberterrorism and expounds on scholarly disagreements about whether cybercrime should be viewed as simply a traditional offense using new tools, or a new, unique form of offense.[13] Compounding the problem, Bryant explains that every

---

[9] Goodman, *Future Crimes*, 22.

[10] Ibid., 465.

[11] Michael Riley et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew it," *Bloomberg*, March 13, 2014, www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

[12] Peter Elkind, "Sony Pictures: Inside the Hack of the Century," *Fortune*, June 25, 2015, http://fortune.com/sony-hack-part-1/.

[13] Thomas J. Holt, "Exploring the Intersection of Technology, Crime, and Terror," *Terrorism and Political Violence* 24, no. 2 (March 14, 2012): 338–340.

law enforcement agency defines cybercrime based on its own unique authorities.[14] While Jarvis, MacDonald, and Nouri write about debate and disagreement surrounding cyberterrorism, Demchak writes about similar lack of consensus concerning the concept and definition of cyberwar.[15] Divergent ideas, exemplified by absent definitional consensus, can create wasted law enforcement effort, the costs of which are substantial, though often unrecognized.

The dark web's complexity is evident in literature that describes its anonymous and disruptive nature. While White explains how the Defense Advanced Research Projects Agency (DARPA) is trying to achieve Internet affordances to curb human trafficking facilitated by the dark web, Goodman explains how criminals are better than most people at adapting to new technologies because they are used to committing crimes in an environment that is constantly in flux.[16] Criminals are using the dark web to facilitate both cybercrime and border-related crimes, such as drug trafficking. Goodman and Maras do a thorough job of explaining how drug trafficking occurred on the Silk Road, an online criminal marketplace in the dark web where drug consumers could order any type of drug through the Internet.[17] According to Maras, the site even provided advice on how not to get caught by advising dealers to avoid shipping orders directly to an individual's residence. Goodman and Maras explain how drugs can be ordered, sold, and shipped anywhere in the world due to the dark web's interconnectivity. This background is important because it exemplifies how the Internet is now facilitating border-related crimes: drugs can be ordered online from anywhere in the world, but still must physically cross U.S. borders to get to consumers.

---

[14] Robin Bryant and Sarah Bryant, *Policing Digital Crime* (Burlington, VT: Ashgate, 2014), 26, 38.

[15] Lee Jarvis, Stuart MacDonald, and Lella Nouri, "The Cyberterrorism Threat: Findings from a Survey of Researchers," *Studies in Conflict & Terrorism* 37 (September 2013); As cited in Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012), 98, 122–128.

[16] "Christopher White: Fighting the 'Dark Web,'" YouTube video, 14:16, from a TedxTalk on the Oklahoma State University campus on April 10, 2015, posted by TEDxTalks, April 30, 2015, https://www.youtube.com/watch?v=9QsjkJcUznA; Goodman, *Future Crimes*, 229–231.

[17] Goodman, *Future Crimes*, 245–250; Marie-Helen Maras, "Inside Darknet: The Takedown of Silk Road," *Criminal Justice Matters* 98, no.1 (December 2014), doi:10.1080/09627251.2014.984541.

2. Border Crimes and Internet Use

Published books, government testimony, and journal articles mostly address physical aspects of border crimes; there is far less material describing how these crimes are facilitated by the Internet. Experts cite multiple reasons for border-related crime, including increased illegal immigration resulting from past immigration policies, the United States' propensity for involvement in various forms of smuggling, and global economics. This review also reveals divergent findings about how the Internet facilitates border-related crimes and whether new technologies negatively impact enforcement.

Andreas' research details the history of increasing border enforcement, and how U.S. policies that seek to deter the illegal movement of people and goods have impacted smuggling.[18] Specifically, he explains how U.S. enforcement strategies have changed regarding the smuggling of drugs and undocumented immigrants from Mexico. Andreas does not agree with political rhetoric that declares the United States has lost control of the border in order to gain political support for greater policing; rather, he believes the United States has never had control of the border. He provides a historical context of smuggling and explains that, by policing the border more, the United States is only heightening the smuggling problem.

Massey, Durand, and Pren corroborate Andreas' claim that increasingly stringent border enforcement policy decisions have negatively impacted undocumented immigration. The authors assert that human smuggling, and dramatic increases of Mexican undocumented immigrants remaining in the United States, are a result of increased border enforcement.[19] This literature explains how human smuggling across the U.S.–Mexico border became a lucrative crime because of immigration policy decisions. The increased border policing moved undocumented immigrant crossings away from easy, established paths to more difficult crossing areas. As an unintended consequence, travelers began hiring human smuggling organizations to help them

[18] Peter Andreas, *Border Games: Policing the U.S.-Mexico Divide*, 2nd edition, Kindle (Ithaca, NY: Cornell University Press, 2009).

[19] Douglas S. Massey, Jorge Durand, and Karen A. Pren, "Why Border Enforcement Backfired," *American Journal of Sociology* 121, no. 5 (March 2016): 1590.

traverse the more difficult terrain, thereby increasing illegal immigration costs, which caused people to stop returning to Mexico.[20]

In addition to providing historical evidence of drug smuggling, the literature also identifies the Internet as a means to smuggle items like intellectual property and pornography. As Andreas explains, the Internet is just another method, like car trunks and luggage.[21] Of particular value for this research, Andreas states that "most smuggling parallels the methods and routes of legal commerce," even when employing the Internet.[22] More recently, Andreas explains how globalization and technology have made both legal and illicit transactions easier and less costly.[23] He explains how border crimes all have some basis in smuggling, and shows how the United States has been historically reliant on smuggling. Border-related crimes are connected to the smuggling of prohibited commodities; legal commodities that wish to avoid sanctions, taxes, or tariffs; stolen or counterfeit commodities; people; and endangered species. Andreas discusses how new technologies such as the Internet have aided criminal activity, but he also asserts that those same technologies have aided enforcement: "We greatly understate the degree to which the same technological transformations that have facilitated the globalization of crime also facilitate the globalization of crime control."[24]

Finklea further discusses the Internet and discusses how cyberspace interacts with border security.[25] She explains how criminal activity is becoming as borderless as legitimate business, through globalization and interstate commerce. Her article discusses the difficulty of maintaining a border in the virtual world and identifies crimes, such as

---

[20] Massey, Durand, and Pren, "Why Border Enforcement Backfired," 1590.

[21] Peter Andreas, *Border Games*, 521.

[22] Ibid.

[23] Peter Andreas, *Smuggler Nation: How Illicit Trade Made America*, Kindle edition (New York: Oxford University Press, 2013), 331–332.

[24] Ibid., 341–345.

[25] Kristin M. Finklea, "The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement," *Journal of Current Issues in Crime, Law and Law Enforcement* 5, no 1/2 (February 2012): 29–67.

fraud and identity theft, that are being re-categorized as non-traditional (rather than traditional) cybercrimes.

3. Affordance Theory, Affordances, and Crime

Affordance theory has been used to explain human actions in the fields of ecological psychology, sociology, strategy, law, and human-computer design. The literature recognizes James Gibson as the architect of affordance theory; he was purportedly the first to write about the concept of affordances, for the field of ecological psychology. Gibson defines affordances as "the complementarity of the animal and the environment."[26] He explains that affordances relate to all of an individual's action possibilities, whether recognized or not, and that humans interpret cues from the environment to determine how to interact with objects.[27]

Norman builds upon Gibson's work by using affordance theory in the study of human–computer interactions. Norman also builds on Gibson's study of perception by developing the term "perceived affordance."[28] He describes perceived affordance as the interaction perceived to be most likely between a human and another object, such as a computer, based on past experiences. Norman's writings are the basis for identifying and understanding affordances in design theory, and a large amount of literature about design theory supports Norman's work.

Robey, Anderson, and Raymond expound on Norman's use of affordances for design theory, explaining it is intended to direct technology designers to make uses of technology obvious: "The affordance relationship exists as long as action possibilities are perceivable, but the relationship remains even when we do not focus on action possibilities."[29] Despite the relevance of Norman's work—which goes a long way to illuminate why people use the Internet for different purposes—the most valuable

---

[26] James J. Gibson, *The Ecological Approach to Visual Perception* (Boston: Houghton Mifflin, 1979), 127.

[27] Norman, *The Design of Everyday Things*, 12.

[28] "Affordances and Design," Nielsen Norman Group, accessed February 19, 2017, www.jnd.org/dn.mss/affordances_and.html.

[29] Robey, Anderson, and Raymond, "Information Technology," 387.

affordance definition, at least in terms of understanding criminal affordances, comes from literature about strategy tools. In discussing strategy tools, Jarzabkowski and Kaplan explain that affordances' "use depends not only on the material properties or on the intended design of the tool, but also on the context and the interpretations of actors who may use the technologies in creative, unpredictable ways."[30] This is significant because it posits that everyone will perceive and possess different affordances, depending on the person's unique relationship to the object.

Use of affordance theory for human–computer design should prove valuable for analyzing Internet-facilitated crimes, but the literature on affordance theory specific to criminal justice, especially border-related crimes, is limited. One study by Gill, Conway, Thornton, Bloom, and Horgan uses affordance theory to study criminal use of the Internet by terrorists. Although their research concludes that the Internet provides affordances to terrorists, it does not determine whether Internet or physical-world experiences create more radicalization.[31] Of most significance is the finding that potential terrorist plotters rely on a hybrid approach of Internet use and physical-world encounters for radicalization. It is this hybrid nature—Internet use combined with physical-world elements—that is central to this thesis.

4. Stigmergy

Stigmergy is a concept that has been used by various disciplines to explain how agents achieve self-organization in decentralized group settings.[32] Zoologist Pierre-Paul Grasse first introduced the concept to explain how termite colonies self-organize.[33] Various researchers have more recently used the concept to explain human and computer behavior, and material production. When describing the creation of product-driven systems architecture, Pannequin and Thomas write, "The key point of stigmergy is that

---

[30] Jarzabkowski and Kaplan, "Strategy Tools-In-Use," 539.

[31] Paul Gill et al., "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology & Public Policy* 16, no. 1 (2017): 99–117.

[32] Remi Pannequin and Andre Thomas, "Another Interpretation of Stigmergy for Product-Driven Systems Architecture," *Journal of Intelligence Manufacturing* 23 (2012): 2589.

[33] Ibid.

there is no direct communication between actors, only indirect communications through cues deposited on the environment."[34] Goldstone, Jones, and Roberts rely on stigmergy to explain how group behavior from earlier actions influences subsequent actions through the formation of pathways.[35] They note that stigmergy is valuable because it can relate the study of pathway formation from purely physical to abstract analysis. Privat combines the concept of stigmergy with phenotropics to explain self-configuration of embedded systems.[36] His journal article discusses how decentralized systems, including computers and robotics, can interlink actions stigmergically and form self-communication from sensor and human stimuli. While this literature shows stigmergy is adaptable to various disciplines and can be used to explain self-organization of various groups, it does not demonstrate use for the study of crime.

The only specific study of crime as it relates to stigmergy is a journal article by Nieto-Gomez, which explores the resilience of the illegal drug supply chain.[37] He explains how U.S. law enforcement actions are influencing drug traffickers to devise new and better drug-smuggling methods, resulting in a resilient supply chain. In making his argument, Nieto-Gomez describes drug trafficking at the U.S.–Mexico border as a self-organizing environment, and government and criminal agents as the influencing decentralized groups. An important part of his argument is the explanation that the stigmergic relationship allows both decentralized groups to send and receive stimuli; it is an iterative process in which groups both act and react to one another.[38] This literature is directly applicable to the study of border-related crime, causal relationships, and innovative technologies.

---

[34] Pannequin and Thomas, "Stigmergy for Product-Driven Systems Architecture," 2587–2599.

[35] Robert L. Goldstone, Andy Jones, and Michael E. Roberts, "Group Path Formation," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 36, no 3 (May 2006):

[36] Gilles Privat, "Phenotropic and Stigmergic Webs: The New Reach of Networks," *Universal Access in the Information Society* 11, no. 3 (2012): 323–335.

[37] Nieto-Gomez, "Stigmergy at the Edge," 31–40.

[38] Ibid.

5. The Silk Road and Silk Road 2.0

The Silk Road and Silk Road 2.0 were two darknet marketplaces that used Internet technologies to facilitate the smuggling of illegal drugs into the United States. Two books, written by Goodman and Bilton, contain particularly valuable information about the Silk Road. While Goodman's material focuses on the Silk Road's technologies and criminal activities, Bilton provides a more personal description of the Silk Road operator and criminal investigation.[39] Goodman explains how the dark web, Tor, and other technologies were used to facilitate criminals who used the Silk Road to smuggle such items as drugs, guns, and stolen credit cards.[40] Bilton's material explains that the operator created the Silk Road based on libertarian ideals, and maps the thought process for how technologies were selected.[41] In addition to Bilton's literature, court documents provide the most information about the criminal activities and law enforcement techniques used to gather evidence.

A search for research about Silk Road 2.0 resulted in less literature. The primary Silk Road 2.0 reference material comes from court documents and online articles and forums. Court documents for the criminal case against operator Blake Benthall explain that Silk Road 2.0 relied on the same Internet technologies as the Silk Road.[42] Court documents also show how the arrest of the original Silk Road operator impacted perceptions of Silk Road 2.0.[43] Court documents for the criminal case against Brian Farrell, the second Silk Road 2.0 operator, provide similar material; additionally, an order written by Judge Richard A. Jones discloses how law enforcement received help overcoming Tor anonymity from Carnegie Mellon University's (CMU) Software Engineering Institute (SEI).[44] This literature is valuable for understanding how

---

[39] Goodman, *Future Crimes*, 194–200; Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* (New York: Portfolio/Penguin, 2017).

[40] Goodman, *Future Crimes*, 245.

[41] Bilton, *American Kingpin*, 33–46.

[42] United States v. Blake Benthall, Sealed Complaint, 1:14-mj-02427-UA (SD NY, October 29, 2014).

[43] Ibid.

[44] United States v. Brian Farrell, Order on Defendant's Motion to Compel, CR15-029RAJ, (WD WA, February 23, 2016.)

technologies were used for Silk Road 2.0 and law enforcement's corresponding adaptation of investigative techniques.

The vast majority of the literature found for this study is relevant, comprehensive, and scholarly. The material about affordance theory helps establish an analytical framework unique to the study of crime. When this material is combined with stigmergy literature, a true understanding of the dynamic environment created by crime and law enforcement is achieved. Material about the Silk Road and Silk Road 2.0 is especially valuable for mapping the criminal evolution of hybrid crime and showing law enforcement's corresponding adaptability. When combined, the literature provides a clear picture of how technology in the criminal environment creates challenges for law enforcement.

D. RESEARCH DESIGN

This thesis analyzes the criminal issue of border crimes facilitated by the Internet, using the Silk Road and Silk Road 2.0 as case studies. I chose the Silk Road and Silk Road 2.0 because both examples have a border nexus, they facilitated crime using Internet technologies, and they maintained both physical and digital criminal elements. This hybrid nature does not allow for neat categorization into physical or cybercrime subsets; I believe this explains why law enforcement was initially unable to detect or respond to newly perceived Internet affordances. The realization that the hybrid nature of certain crimes creates difficulties for criminal typology and response became a central part of this research.

After identifying and selecting these two cases, I gathered pertinent data on how criminal actors traditionally commit border-related crimes; the investigative techniques law enforcement traditionally employs; how the criminal actors in these examples used the Internet to commit the criminal activity; how law enforcement identified the criminal activity facilitated by the Internet; what law enforcement did to overcome the criminals' Internet affordances; and the traditional or new investigative techniques used to gather evidence. I analyzed the resulting data using affordance theory and the concept of stigmergy as frameworks.

In doing so, my intention was to identify the differing Internet affordances between criminal actors and law enforcement pertaining to drug trafficking, human trafficking and sexual exploitation, and money laundering. I also initially believed that a wide technology gap exists between criminals and law enforcement which does not allow for general criminal deterrence, even when criminal investigations lead to arrests. When arrests are made for crimes facilitated by the Internet using only traditional law enforcement techniques, rather than narrowing the technology gap by realizing criminal Internet affordances, it allows criminals to believe criminal methods are still effective. If criminals still believe the Internet can facilitate future crimes, any arrest made will only be a specific, as opposed to a general, deterrence. I therefore believed that general deterrence is not possible without eliminating the technology gap between law enforcement and criminals.

The actual output of the research, however, was a mixture of validation, invalidation, and inconclusiveness. I did find that criminals and law enforcement realize different Internet affordances in their perception of border-related crime. However, contrary to my initial belief, and despite validating that criminals and law enforcement have different Internet affordances, I found that a wide technology gap does not exist. Finally, the output relative to deterrence was inconclusive. I found that traditional and unconventional investigative techniques were both effective at achieving specific deterrence, but neither has achieved general deterrence.

II. THE INTRODUCTION OF A HYBRID CRIME

> The value of a well-designed object is when it has such a rich set of affordances that users can do things with it that the designer never imagined.
>
> —Donald Norman[45]

In 1859, Charles Darwin opened people's eyes to the concept of evolution when he published the book *On the Origin of Species by Means of Natural Selection*.[46] According to George Levine, Darwin theorized that organisms' "perpetuation through heritability is largely determined by their usefulness in adapting the organism to its environment."[47] As part of his explanation of evolution, Darwin discusses the hybridization of organisms and difficulties in predicting hybrid organism sterility and fertilization.[48] While Darwin's research focuses on understanding changes to living organisms, evolution and hybridization can also be used to explain many non-biological changes in society, including crime. Crime and deviant behavior are social constructs that continually adapt to the environment and *evolve*. Similar to biological organisms, crime can hybridize as part of an adaptive survival process. Recently, cross-border crimes have adapted to environmental pressures and evolved; while they were once traditional, physical crimes, they now contain both physical and digital elements. Evolution has bred a new hybrid crime category that has changed the typology of crime.

Advancements in Internet technologies have made cross-border hybrid crimes possible.[49] While criminal transformation might be seen as a natural social evolution of

---

[45] "Models and Theories in Human-Computer Interaction/Norman's Affordances-Visibility and the 7 Stages of Action," WikiBooks, accessed December 6, 2017, https://en.wikibooks.org/wiki/Models_and_Theories_in_Human-Computer_Interaction/Norman%27s_Affordances_-_Visibility_and_the_7_Stages_of_Action.

[46] Charles Darwin, *The Origin of Species by Means of Natural Selection* (Annotated), Kindle edition (G. Books, 2011), 82.

[47] Darwin, Introduction, 442.

[48] Darwin, Chapter VIII, 108–115.

[49] Finklea, "The Interplay of Borders," 29.

deviant behavior, Internet technologies have introduced a "game-changing" adaptation. They have dramatically disrupted the understanding of criminal activity and forced law enforcement into a realm normally occupied by technology experts. Understanding hybrid crimes requires a new mindset and new theories of evaluation. Further, preventing, disrupting, and prosecuting these hybrid crimes requires new investigative tools based on specialized technical expertise. This chapter identifies the pressures that caused hybrid crime to form, uses the concept of stigmergy to explain the dynamic relationship between criminal activities and law enforcement actions, and proposes affordance theory as an unconventional method for analyzing criminal transformations facilitated by Internet technologies.

A. WHAT IS HYBRID CRIME?

Drug trafficking, human trafficking/sexual exploitation, and money laundering are cross-border crimes that have evolved to include physical and digital elements. Border-related smuggling may be committed using various means and methods. Traditional methods rely on the physical movement of goods or people, cash payments, and in-person meetings. Some smuggling still relies exclusively on physical objects and physical actions, but now other methods exist in the digital realm. Cross-border crimes may still be purely physical or purely digital, but the ones that are being viewed for this study are a hybridization of the two. The hybrid nature of these crimes does not result in a new crime, but in a new category of crime and changed criminal typology.

For purposes of this study, I define a hybrid crime as one that relies on both physical and digital elements, and each element has to fulfill a critical part of the activity to accomplish the overall crime. One way to better understand how the new hybrid category impacts criminal typology is by comparing different categories of crime. The following hypothetical examples demonstrate different categories of crime for smuggling child pornography through a U.S. international airport.

(1) Physical Crime Category

A person can smuggle hard-copy images of child pornography into the United States by concealing them in a suitcase. In this example, law enforcement can locate the

illegal contraband using the traditional physical technique: inspecting the suitcase. From this physical action, law enforcement can identify that a crime has been committed. In this purely physical crime, the object is physical, and the action of crossing the border with concealed illegal contraband is also physical.

(2) Digital Crime Category

A person outside the country can use the Internet to "smuggle"—through file sharing—digital images of child pornography to someone in the United States. The images are never printed and remain digital. If law enforcement had information that illegal contraband was being smuggled through a particular email account, they could obtain an email search warrant. From this warrant, officers could identify that a crime is being committed; then, if the criminal travels to the United States, he could be arrested. This is a cybercrime because the object is digital, and the action of sending the digital object through the Internet is also digital.

(3) Hybrid Crime Category

A person can smuggle digital images of child pornography into the United States by downloading them from the Internet while in a foreign country, and then transporting the saved digital images across the U.S. border on a laptop or mobile telephone. In this instance, law enforcement can locate the illegal contraband using the traditional cybercrime technique: creating an image of the laptop and telephone to inspect the devices, thus exposing the crime. This is a hybrid crime because the object is digital while the action of crossing the border with illegal contraband is physical.

(4) Undetermined Crime Category

A person can "smuggle" digital images of child pornography into the United States that are saved electronically in a cloud-based file-sharing service such as Dropbox or IDrive. Law enforcement could create an image of the laptop and telephone to inspect for illegal contraband; however, in this example, law enforcement might not be able to identify the images or even the file-sharing account. The traditional law enforcement technique (physical inspection) or cybercrime technique (imaging devices) would not

identify the illegal contraband. The crime could be categorized as a cybercrime if the images are downloaded from the Dropbox or IDrive, thus rendering them into a digital format. It could also be categorized as a hybrid crime because the accounts or images are saved digitally, albeit in the cloud, and the person is physically entering the United States. The complication with labeling this example crime is that even though the person is physically entering the United States, the images are not being physically or digitally smuggled until they are downloaded from the cloud. This example crime is difficult to classify because the actions and the objects do not fit neatly within physical, digital, or hybrid categories.

These hypothetical examples show the complexity of crime and how difficult it can be to determine proper classifications. They also show that pure categories are rare and most crime has some degree of crossover. It is the degree of crossover that helps determine whether a crime has evolved into a new classification, which is how the "hybrid crime" classification was created. The label of "hybrid" would never have come to fruition for border-related crime if it were not for various social, environmental, and technological pressures. The next section explains those pressures that caused cross-border crime to evolve into hybrid crime.

B. CROSS-BORDER CRIME: RIPE FOR TRANSFORMATIVE CHANGE

Committing crime is similar to all other high-risk activities; criminals always attempt to take the easiest path to success. The easiest path will always be the natural course of action among many possible courses. Although there are legal high-risk activities, such as initiating a start-up company, criminal actions carry the highest risks. A failed start-up company might result in financial ruin, but failure to successfully commit a criminal act can lead to long-term incarceration or even death. Consequently, criminals are always looking for new paths through with to commit new, unique crimes, or to commit old crimes in unique ways.

Technological innovations disrupt the law enforcement–crime balance in much the same way that they disrupt the business economy. According to an article about disruption for entrepreneurship, "when you're disrupting an industry, you can focus on

end goals without having to follow a traditional path."[50] The same can be said about crime. When a criminal uses a technology for the first time to facilitate a crime, it disrupts the law-and-order balance and makes it difficult for law enforcement to respond adequately.[51] Following a predictable pathway to commit crime makes it relatively easy for law enforcement to identify the crime and respond, especially if the criminal uses physical elements. When technology enters the equation, it changes known objects and therefore the predictability of actions that stem from those objects. Criminal use of innovative technologies can thus render law enforcement techniques ineffective.

Disruption can occur in business or crime only if the environment is ripe for transformative change.[52] Cross-border crime was ripe for change due to three pressures. This pressure first came about from increased enforcement against cross-border smuggling, which caused criminals to search for alternative techniques to commit crime. Enforcement pressure was supported, second, by Internet technologies that were found to fulfill elements of the criminal activity; criminals began to implement the technologies to overcome the increased border enforcement efforts. Third, the technologies proliferated among criminal consumers because of a changing popular mindset that Web-based social networks offer a sense of community and trust. The end result (as shown in Figure 1) was the creation of a hybrid category for cross-border crime.

---

[50] Rob Biederman, "5 Secrets to Recognizing an Industry Ripe for Disruption," *Entrepreneur*, August 4, 2014, https://www.entrepreneur.com/article/235881.

[51] Finklea, "The Interplay of Borders," 43.

[52] William D. Eggers, *Delivering on Digital: The Innovators and Technologies that Are Transforming Government*, Kindle edition (New York: Rosetta Books, 2016), 100–143.

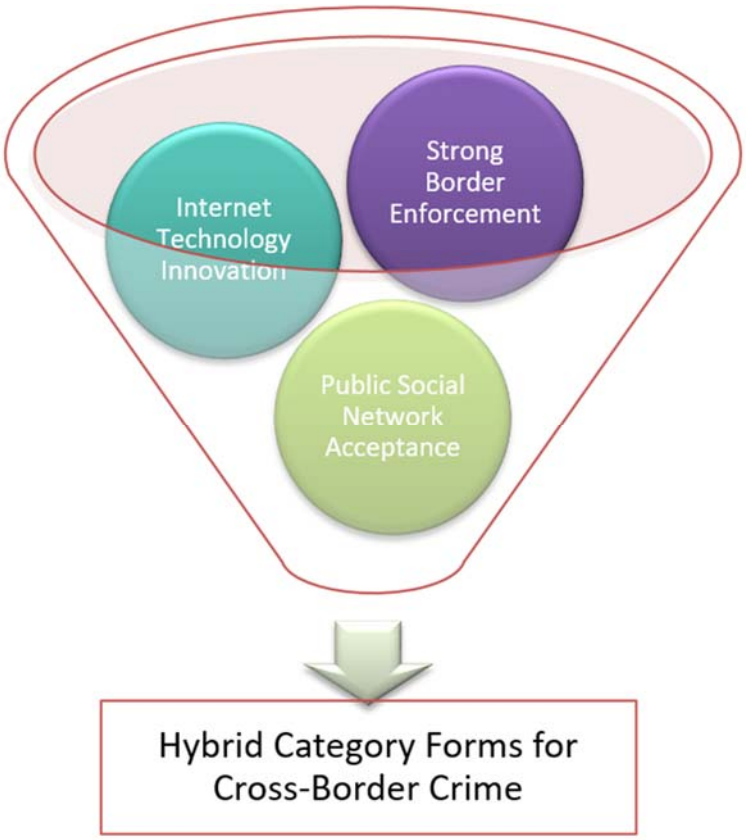

Figure 1. Combined Pressures Create Hybrid Crime

1. Pressure from Strong Border Enforcement

The United States made border security an enforcement priority long before "build the wall" became an iconic phrase. Over the years, border security efforts have focused variously on illegal immigration, drug smuggling, and terrorism. Starting in 1986, the United States dramatically increased the amount of resources expended on reducing the flow of illegal immigrants coming into the United States across the Mexico border.[53] From 1993 to 1999, the Immigration and Naturalization Service's budget nearly tripled.[54] A large part of that budget was spent on increasing the number of Border Patrol

[53] Massey, Durand, and Pren, "Why Border Enforcement Backfired," 1569.

[54] Andreas, *Border Games*, 2334.

agents at the southern border, from 3,389 to 8,200.[55] Another portion of the budget was used to purchase technology, including cameras, sensors, and night vision goggles.[56]

The war on drugs was another source of pressure exerted on cross-border criminal activity. This "war," which started in the 1960s, increased enforcement resources throughout various administrations for decades and uniquely included law enforcement, military, and intelligence assets.[57] From 1964 to 1968, the U.S. Customs Service achieved increased marijuana seizures from 7,000 pounds to 65,000 pounds.[58] From 1981 to 1989, federal cocaine seizures increased from two tons to one hundred tons.[59] The increase in resources to stop the Colombian cocaine trafficking problem in south Florida resulted in pushing criminal activity from Florida to the U.S.–Mexico border.[60] The interlinking of Colombian traffickers with Mexican traffickers created new criminal networks and resulted in even more enforcement resources being expended to stop the flow of drugs.[61]

When the Department of Homeland Security was created after 9/11, border enforcement was again strengthened by two new agencies: U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). CBP was created for interdiction of cross-border crime. As part of CBP, the U.S. Border Patrol grew the most after 9/11; in 2003, the USA PATRIOT Act increased Border Patrol's budget by $300 million.[62] The Secure Fence Act provided funding for an additional 3,000 Border Patrol agents and another $244 million budget increase in 2006.[63] As of 2016, CBP had a $13.3 billion budget and grew to approximately 59,000 employees; in the same fiscal year, the

---

55 Andreas, *Border Games*, 2334.

56 Ibid.

57 Andreas, *Smuggler Nation*, 253, 272–273, 275, 281, 284.

58 Ibid., 273.

59 Andreas, *Border Games*, 988.

60 Andreas, *Smuggler Nation*, 334.

61 Andreas, *Border Games*, 1026–1046.

62 Massey, Durand, and Pren, "Why Border Enforcement Backfired," 1569.

63 Ibid.

Border Patrol made 415,816 apprehensions, while CBP officers arrested 8,129 people for serious crimes and stopped 274,821 inadmissible aliens from entering the United States at ports of entry.[64] CBP also seized over 2.9 million pounds of narcotics, $105 million in currency, and 733 outbound weapons.[65]

ICE was created to conduct investigations and interior enforcement designed to strengthen border security by focusing on transnational crimes. Like CBP, ICE has also seen significant growth since its creation after 9/11. As of 2016, ICE had a $6.2 billion budget and approximately 20,000 employees.[66] For fiscal year 2016, ICE's Homeland Security Investigations (HSI) made 32,709 criminal arrests and 6,544 administrative arrests while ICE's Enforcement and Removal Operations removed 240,255 illegal aliens from the United States.[67]

It is difficult to measure the effectiveness of these efforts, and doing so is not the focus of this thesis. What matters for this study is that there has been a dramatic increase in border enforcement that has created pressure on cross-border crime. That pressure forced criminal actors to adapt. Adaptation led to a search for alternative means to commit crime and the discovery that certain Internet technologies could facilitate criminal actions. The following section explains the Internet technology innovations that helped cross-border crime evolve into hybrid crime.

2. Pressure from Internet Technology Innovations

While enforcement efforts were making smuggling more difficult, technological advances simultaneously expanded options for criminal activity. Criminals operate in a mindset that distancing themselves from the physical elements of criminal activity give them a better chance of eluding arrest. In the past, that distance was created by using

64 "FY 2018 Budget in Brief," Department of Homeland Security, accessed December 1, 2017, 11, 25, 26, https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf.

65 Ibid., 24–25.

66 Ibid., 11, 32.

67 Ibid., 33.

third-party proxies to commit physical crimes. Today, the Internet has become the proxy, effectively creating distance between crime and physical actions.

The Internet has been used for many years as a platform to commit pure cybercrimes involving fraud, theft, and extortion through distributed denial of service attacks, spear phishing, spam, ransomware, or malware.[68] However, using the Internet to facilitate traditional physical crimes like drug trafficking, human trafficking and sexual exploitation, and money laundering is a much newer phenomenon. This phenomenon has only become possible because of developments such as Tor, cryptocurrencies, tumblers, and peer-to-peer file transfer protocols. These technological innovations have allowed communications, digital file transfers, and money transactions to occur anonymously on the dark web. Once these new technology innovations were discovered, it was a small leap to perceive additional criminal uses for the Internet and to form hybrid crime.

The onion router Tor has made the dark web a place where deviant behavior remains anonymous. Tor is software designed to anonymize user identities by routing communications through various nodes on a worldwide network in a way that does not permit sources or destinations to see one another.[69] Tor software also allows for hidden website development in the deep web.[70] Tor was developed in collaboration with the Naval Research Laboratory, DARPA, and the Massachusetts Institute of Technology to allow the U.S. military to securely communicate with foreign intelligence and military assets overseas.[71] Released to the public in 2004, Tor has been used legitimately by individuals or businesses who wish to protect personal identities while conducting competitive research, by activists and whistleblowers who report abuses, and by journalists who wish to consult sensitive sources.[72]

---

[68] Reveron, *Cyberspace and National Security*, 64.

[69] Goodman, *Future Crimes*, 198.

[70] Ibid.

[71] Jeff Stone and Charles Poladian, "Meet the Deep Web: Inside the Hidden Internet that Lies beyond Google," *International Business Times*, December 31, 2014, http://www.ibtimes.com/meet-deep-web-inside-hidden-Internet-lies-beyond-google-1725784.

[72] "Tor," Tor Project, accessed November 18, 2017, https://www.torproject.org/index.html.en.

Hybrid crime is difficult to commit without the ability to anonymously transfer money. Cryptocurrencies were the technological solution to that problem. Bitcoin is a virtual cryptocurrency that was introduced in 2009 based on a white paper written by an author using the pseudonym Satoshi Nakamoto.[73] Bitcoin uses peer-to-peer transactions that do not require a third party to process monetary transactions.[74] Transactions are pseudo-anonymous because users and Bitcoins are encrypted and rely on cryptography to validate transactions, but are recorded on a public ledger called a blockchain.[75] Bitcoin was invented so transactions on the Internet could be "based on cryptographic proof instead of trust," which allows for decentralized payments outside financial institutions.[76] A Bitcoin tumbler helps make transactions more anonymous by manipulating the blockchain, which obfuscates the path between a "buyer's Bitcoin address and the vendor's Bitcoin address."[77]

Peer-to-peer file transfer protocols allow users to transfer large amounts of data through the Internet. BitTorrent is an example of an open-source protocol that allows big data to be segmented into smaller components, transferred through a peer-to-peer network, and then reassembled.[78] BitTorrent has been used for legitimate transfers of large amounts of information by Facebook, Twitter, Florida State University, and Blizzard Entertainment.[79] However, criminals have found that when BitTorrent is combined with other technologies, transfers can be made pseudo-anonymously.[80] As a

---

[73] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, accessed December 1, 2017, https://bitcoin.org/bitcoin.pdf.

[74] Craig K. Elwell, M. Maureen Murphy, and Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, CRS Report No. R43339 (Washington, DC: Congressional Research Service, 2015), 3.

[75] Ibid.

[76] Nakamoto, "Bitcoin."

[77] United States v. Ross William Ulbricht, Sealed Complaint, 13 MAG 2328, (SD NY, September 27, 2013), 14.

[78] Jessi Hempel, "The Inside Story of BitTorrent's Bizarre Collapse," *Wired*, June 19, 2017, https://www.wired.com/2017/01/the-inside-story-of-bittorrents-bizarre-collapse/.

[79] Ibid.

[80] Ibid.

result, criminals have used BitTorrent protocol to transfer pirated movies, music, software, and child pornography.[81]

The technologies of Tor, cryptocurrencies, tumblers, and peer-to-peer file transfer protocols have made the Internet valuable for facilitating cross-border crime. While none of these technologies were specifically designed for the purpose of committing crime, their development and subsequent criminal discovery impacted the criminal environment and made hybrid crime possible. When criminals realize these technologies' values, the combined pressure from increased border enforcement created a market that was ripe for transformative change. The final pressure that allowed hybrid crime to flourish in this emergent environment was social acceptance. The next section explains how social network acceptance legitimized darknet marketplaces in the public mind.

3. Social Network Acceptance

One of the most significant impacts the Internet has had is the creation of virtual communities through social network services like Facebook, Myspace, and Twitter.[82] These types of social networks have connected hundreds of millions of people into virtual communities of like-minded individuals.[83] The individuals feel they are part of the community by having forum discussions that help build virtual bonds. Although these bonds are merely virtual, they create a sense of social acceptance and trust.

Media dependency theory explains why people support social networks; the theory proposes that there exists "an internal link between media, audience and large social system[s]."[84] As individuals rely more and more on their media platforms in order "to comprehend and understand the world around them," they build trust in those

---

[81] Duncan Graham-Rowe, "Sniffing Out Illicit BitTorrent Files," *MIT Technology Review*, October 22, 2012, https://www.technologyreview.com/s/412021/sniffing-out-illicit-bittorrent-files/.

[82] Hsin-Yi Huang, Po-Lin Chen, and Yu-Chen Kuo, "Understanding the Facilitators and Inhibitors of Individual's Social Network Site Usage," *Online Information Review* 41, no. 1, (2017): 85.

[83] Ibid.

[84] "Media Dependency Theory," Communication Theory, accessed November 18, 2017, http://communicationtheory.org/media-dependency-theory/.

platforms.[85] Individuals also build relations into the social network through dependencies of understanding and orientation.[86] While dependency of understanding relies on community support to explain "one's own beliefs," dependency of orientation explains how people behave in various social relationships.[87] As people became more dependent on the Internet as a medium and on social networks as communities, darknet marketplaces were a natural progression—an extended community of trusted virtual "friends."

The popular mindset that supports social networks on the Surface Web transferred the same sense of belonging, social comfort, and trust to darknet marketplaces. Dark networks are a component of darknet marketplaces and an extension of accepted social networks from the Surface Web. Like social networks on the Surface Web, dark networks build virtual social communities. The difference between Surface Web and dark web social networks is the level of secrecy and anonymity. Dark web networks allow for discussions and activities that are normally considered deviant to be conducted anonymously. Forum discussions could include questions about illegal drug use, where to obtain certain drugs, or how to locate child pornography. The connections these networks facilitate are significant; in 2015, a researcher found that "just one Dark website alone had more than twenty-seven thousand registered pedophile members in its forums."[88] By fostering online reputation systems, darknet markets have also been extremely successful at building an online community of trust.[89]

Surface Web and dark web social networks have the same output: they grow virtual social communities of like-minded individuals through engagement. Trust in these virtual communities is a strong motivator for members who decide to use technology to commit crime. Once a person is a part of the virtual community, that person trusts the

---

[85] Maureen Syallow, "Media Dependency Theory in Use," Academia.edu, accessed November 18, 2017, http://www.academia.edu/9834996/Media_Dependency_Theory_in_Use.

[86] Huang, Chen, and Kuo, "Facilitators and Inhibitors," 87.

[87] Ibid.

[88] Goodman, *Future Crimes*, 206.

[89] Ibid., 195.

other community members and the technology to protect his identity. Through discussions and online observations, those who are inclined to commit crime are motivated to use the trusted technology to do so. This has become the new normal for committing crime.

In summary, environmental, technological, and social pressures have combined to transform cross-border crime into a new hybrid category of crime. In itself, a new category is just a label used to determine typologies of crime; a changed label would not matter if it did not directly impact law enforcement. In this case, however, the new category affects law enforcement's real-world understanding of cross-border crime. It has also impacted the effectiveness of known enforcement techniques. Better hybrid criminal methodologies have resulted in criminal activity that is difficult to identify and deter. It is important to understand the causal relationship between law enforcement and criminal activity to grasp the real-world consequences of these criminal adaptations. Only once this relationship is understood can law enforcement analyze actions and reactions to possibly predict future changes in criminal activity. The relationship between law enforcement and criminal activities is explained further in the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THEORETICAL FRAMEWORKS AND CONCEPTS

> If the affordances of a thing are perceived correctly, we say that it looks like what it is. But we must, of course, learn to see what things really are—for example, that the innocent-looking leaf is really a nettle or that the helpful-sounding politician is really a demagogue. And this can be very difficult.
>
> —James J. Gibson[90]

A. WHY HYBRID CRIME WAS CREATED: STIGMERGY

Which came first, the *chicken or the egg*? This causality dilemma is intended to make us think about how two objects that have a causal relationship came into being. Deviant behavior and criminal justice, too, have a rife causal relationship; it is unknown how each influences the other. This makes it difficult to determine if new crime originates on its own or out of a response to enforcement activity. Perhaps it does not matter whether the chicken or the egg came first. But it does matter whether criminal enforcement of crimes initiates new or emergent criminal activities; this determination may help law enforcement reflect on results, identify unintended consequences, or even anticipate future crimes. Crime and law enforcement's causal relationship—and its which-came-first dilemma—is the start of a bigger discussion about how all actions within a causal relationship have reactions.

The actions and reactions between crime and law enforcement can be further explained by another metaphor: *the cat and the mouse.* Like the *chicken or the egg*, the *cat and the mouse* metaphor is also commonly used to explain the relationship between law enforcement and criminals. The cat and mouse have a causal relationship in which they entice actions from one another in a game that continues indefinitely. Law enforcement (the cat), is constantly trying to catch the criminal (the mouse), in a "game" of law and order. Both metaphors can help explicate a concept central to this research that explains how hybrid crimes came about. That concept is stigmergy.

---

90 Gibson, *Ecological Approach*, 142.

Stigmergy, in terms of crime and law enforcement, is very much a combination of the aforementioned metaphors. Stigmergy is a concept meant to explain how agents, including human beings, achieve self-organization in decentralized group settings.[91] As previously mentioned, the concept was first introduced in 1959 by zoologist Pierre-Paul Grasse, who used the study of ethology to explain how termites self-organize to create complicated termite mounds.[92] By studying termites, Grasse concluded stigmergy was the "indirect communication mediated by modifications of the environment."[93] He concluded termites leave a pheromone that directs the colonies' cooperative actions.[94] Since first introduced, stigmergy has been used to explain nest building, animal swarming, physical human movement in the formation of pathways, evolution of software development, product-driven systems in manufacturing, and sensor-driven networks.[95] In these examples, stigmergy has been used to explain actions and reactions in complex relationships that could not otherwise be explained.

Stigmergy is not commonly used to explain the complex relationship between criminal activity and law enforcement, and it has not previously been used to specifically explain the creation of a new category of crime. In a criminal justice context, stigmergy has been used to explain how drug smuggling has become resilient, in part because of the adversarial cycle of law enforcement and drug smugglers in the border setting.[96] Rodrigo Nieto-Gomez explains how enforcement against drug smuggling has created inadvertent resilience in the illegal drug supply chain.[97] He posits that human interactions between criminal and law enforcement activities create indirect indicators that influence one

---

91 Pannequin and Thomas, "Stigmergy for Product-Driven Systems Architecture," 2589.

92 Ibid.

93 Leslie Marsh and Christian Onof, "Stigmergic Epistemology, Stigmergic Cognition," *Cognitive Systems Research*, 9 (2008): 137.

94 Ibid.

95 Goldstone, Jones, and Roberts, "Group Path Formation"; Wei Zhang et al., "Stigmergy-Based Construction of Internetware Artifacts," *IEEE Software* 32, no. 1 (January/February 2015): 58–66; Pannequin and Thomas, "Stigmergy for Product-Driven Systems Architecture"; Privat, "Phenotropic and Stigmergic Webs."

96 Nieto-Gomez, "Stigmergy at the Edge."

97 Nieto-Gomez, "Stigmergy at the Edge."

another.[98] In other words, if law enforcement uses a new enforcement technique that effectively counters certain criminal activity, that action sends out an indirect signal for criminals to adapt their criminal activity. In reverse, if criminals devise new ways to commit criminal activity, that action sends an indirect signal for law enforcement to adapt enforcement efforts.

Nieto-Gomez's research provides a viable explanation for how these indirect signals build resilience within criminal networks, and identifies technology innovation as a way to "shock" the system to impact the cat-and-mouse game.[99] For this study, Nieto-Gomez's most important finding relates to the continuous cycle of criminal activity—how criminal activity influences change for law enforcement, and how law enforcement in turn influences change for criminal activity. The indirect signals flow in both directions, effecting change for both decentralized groups.[100] Stigmergy identifies actions and reactions in the cycle but, despite this valuable advancement, does not answer the chicken-or-the-egg question. This is still an important question; determining whether a specific enforcement technique causes criminal activity to change, or whether criminal activity causes law enforcement to react, helps determine proactive or reactive law enforcement efforts. Determining which came first could also help predict changing typologies of crimes.

Given the stigmergic cycle of law enforcement and crime, it is clear that hybrid crime was created when criminals faced increasing difficulties committing border-related crimes using traditional means. The starting point of the cycle, however, is difficult to determine. Did law enforcement efforts push criminals toward Internet technologies, or did criminal actors simply seek innovation on their own? The cause-and-effect dilemma is compounded by criminal or enforcement activities that do not leave signals on the Internet, as they do in the physical realm. What is known is that when drug smuggling moved from a purely physical crime to a crime that combined physical and digital elements, enforcement became more difficult. The new hybrid crime category forced law

98 Ibid., 3–5.

99 Ibid., 1–3, 11.

100 Ibid.

enforcement to adapt and to advance their understandings of Internet technologies to match the threat.

Stigmergy is a perfect concept for explaining the constant cat-and-mouse cycle of law enforcement and crime, but it does not help predict future crimes. It can only predict that *there will be* future crimes. Affordance theory, on the other hand, offers law enforcement both prospective and ex post facto analysis of criminal activity in greater granularity. Because affordance theory can innovatively perceive action–object possibilities of Internet technologies, it shows promise for predicting future crimes. The next section explains how affordance theory is valuable for analyzing hybrid crimes and how it may help law enforcement predict future crimes.

B. AFFORDANCE THEORY: THE ANSWER TO THE ANALYSIS

1. Affordance Theory, Law Enforcement, and the Internet

The use of Internet technologies to commit criminal activity has made it increasingly important to expand the study of criminal justice and criminology. Traditional reliance on sociology is beneficial for understanding deviant behavior, but it does little to advance investigative techniques capable of stopping hybrid crimes. The theory of affordances has been used extensively in designing digital and physical objects and can be valuable in the analysis of criminal activity. The value lies in the theory having the ability to analyze digital and physical actions equally. As traditional crimes hybridize physical with digital elements, the value of the theory becomes even more important. Affordance theory is ideally suited to advance the fields of criminal justice and criminology by analyzing hybrid crimes.

Affordance theory has not been used to assess crime, so important concepts must be extrapolated from other fields of study. Design theory is a good place to start; affordances have been studied extensively to advance development of physical and digital objects. Design theory requires an understanding of affordances to create physical and digital objects that have obvious uses. Designers want to create objects that are easy

to use and that function as intended.[101] Criminal justice can benefit from affordance theory, in contrast, by using it to identify action–object possibilities that might facilitate crime. If law enforcement is able to identify and understand these affordances, it will be better equipped to respond to objects' new criminal uses.

Design theory helps explain how affordances factor into the causality relationship between an object and the way someone uses that object to perform an action.[102] In the simplest of terms, an affordance is "a relationship between the properties of an object and the capabilities of the agent that determine just how the object could possibly be used."[103] For instance, a shovel is typically used to dig a hole (affords being thrust into the dirt), but can also be used to bludgeon someone (affords being swung). These actions allow a person to employ the shovel's intended use, thrusting to dig a hole, but also an unintended use, swinging to exert blunt force trauma and potentially commit murder. Though graphic, this example illustrates how a physical object's perceived affordances can lead to an unintended use. While objects' intended uses are obvious, determining their unintended uses requires creative insight.

As with violent crimes, criminals may commit cross-border crimes with the help of everyday objects. For example, a gas tank is normally used to store gasoline for fueling a vehicle; a drug trafficker, however, can use a gas tank to store and conceal bricks of cocaine. A tractor trailer can transport produce from Mexico to the United States, but it can also be used to smuggle illegal aliens across the border. Physical action–object relationships are easy to comprehend because they are tangible, but not all action–object relationships are as readily discernable.

The digital realm holds just as many action–object relationships as the physical realm, but they are more difficult to illuminate—which is one challenge law enforcement faces as criminals increasingly employ digital objects to facilitate cross-border crimes. As an example, a computer can be used to create and store spreadsheets that document

---

[101] Norman, *The Design of Everyday Things*, 4–12.

[102] Ibid., 11.

[103] Ibid.

business profits or losses, but a computer can also be used to smuggle digital intellectual property from the United States to China. Most of the world uses the Internet for social communications, personal business transactions, and government and private-sector business functions. But criminals can inject viruses into the Internet that are capable of stealing personal information or affecting the operability of a company's network. Because the Internet affords communication for both criminal and noncriminal purposes, with equal ease, there are many possible Internet affordances to facilitate criminal activity.

As stated previously, once an individual recognizes the Internet's criminal potential, the unique affordances abound; it is only a matter of creativity to find the easiest pathway to success. Design theory uses a concept called "natural mapping" to identify a spatial association between an object and what the object does.[104] While natural mapping in design theory's traditional sense leads to obvious results—e.g., *push this button and this object moves*—natural mapping of the Internet is more abstract. Those who possess the creativity to understand and appreciate the Internet as a complex system of systems can manipulate the positive attributes of borderless communication, unlimited commerce, and most recently anonymity, by visualizing a map for how the Internet can facilitate crime. As with physical natural mapping, individuals with unique digital mapping abilities can identify a digital spatial realization on the Internet: *if I push this button, this result will occur.*

It is important for law enforcement to predict technologies' action–object relationships that lead to crime, or how Internet technologies may be mapped to transform crime. It is possible for anyone to predict action–object relationships; after all, "the affordance of something does not change as the need of the observer changes. The observer may or may not perceive or attend to the affordance, according to his needs, but the affordance, being invariant, is always there to be perceived."[105] In other words, criminals do not own the rights to unlocking new technological keys. Internet technology

---

[104] Norman, *The Design of Everyday Things*, 22.

[105] Gibson, "Ecological Approach to Visual Perception," 138–139.

affordances are omnipresent: anyone can perceive them at any time. Law enforcement and criminals have equal opportunity to perceive and identify Internet affordances. One way to examine predictive actions in order to identify crime is through modeling. The following section explains the *seven stages of action*—a model that can be used for predicting crime.

2. Modeling of Criminal Actions

Don Norman uses a model called the seven stages of action (shown in Figure 2) to determine human actions for design theory.[106] While there is no set beginning or ending point for the model, its concluding point is the accomplishment of a certain goal. After identifying a goal, the stages of execution run through planning, specifying the action(s) needed, and performing. Once those actions are taken and they interact with the environment, a person can evaluate the results. The evaluation has three steps: perceiving how the environment impacts actions, interpreting how the action interacts with the environment, and finally comparing the action outcome against its goal.

[106] Norman, *The Design of Everyday Things*, 40–41.

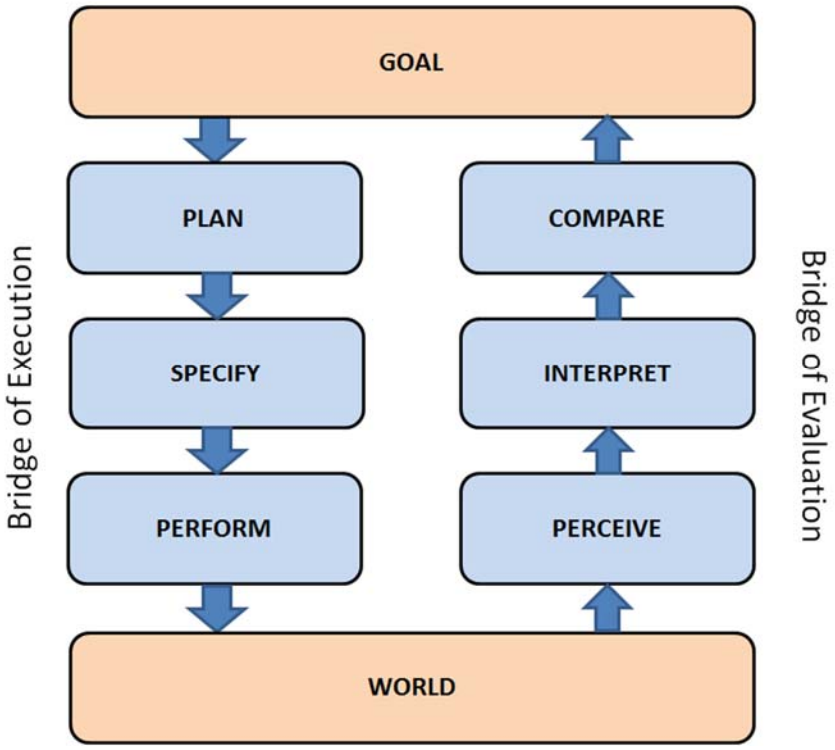

Figure 2. Norman's Seven Stages of Action[107]

Norman uses a simple example to explain the model: he describes how a person determines, plans, and ultimately moves a switch to turn on a light; however, the seven stages can also prove beneficial for modeling criminal actions—specifically, how technology can be used to commit crime.[108] The benefit for this study is in the inverse analysis. The goal of using the seven stages of action is not to design a product (technology) that is user friendly, but rather to reverse-engineer technology to predict how it might be used in the future to commit crime. It might also allow predictive power to determine when a crime is ripe for transformative change.

Figure 3 is an adaptation of Norman's model showing cross-border crime actions resulting in hybrid crime. The model was populated using the Silk Road as a case study. The goal for criminals who used the Silk Road was to "commit cross-border crime." The bridge of execution moved through perceiving digital affordances for crime; specifying

[107] Source: Norman, *The Design of Everyday Things*, 40–46.

[108] Norman, *The Design of Everyday Things*, 40.

the digital and physical elements of the dark web, Tor, Bitcoin and the U.S. Postal Service; and implementing a darknet marketplace. Once those actions interacted with real-world pressures, the model moved into the evaluation stage. The bridge of evaluation demonstrates how the increased border enforcement influenced actions toward the goal. Criminals perceived a high risk for committing border-related crime; they interpreted this risk by recognizing the need for anonymity, which could distance them from physical criminal actions, and by recognizing that hybrid crime is the best option for achieving the goal. In the case of the Silk Road, the actions were extremely effective for accomplishing the goal and ultimately creating hybrid crime.[109]

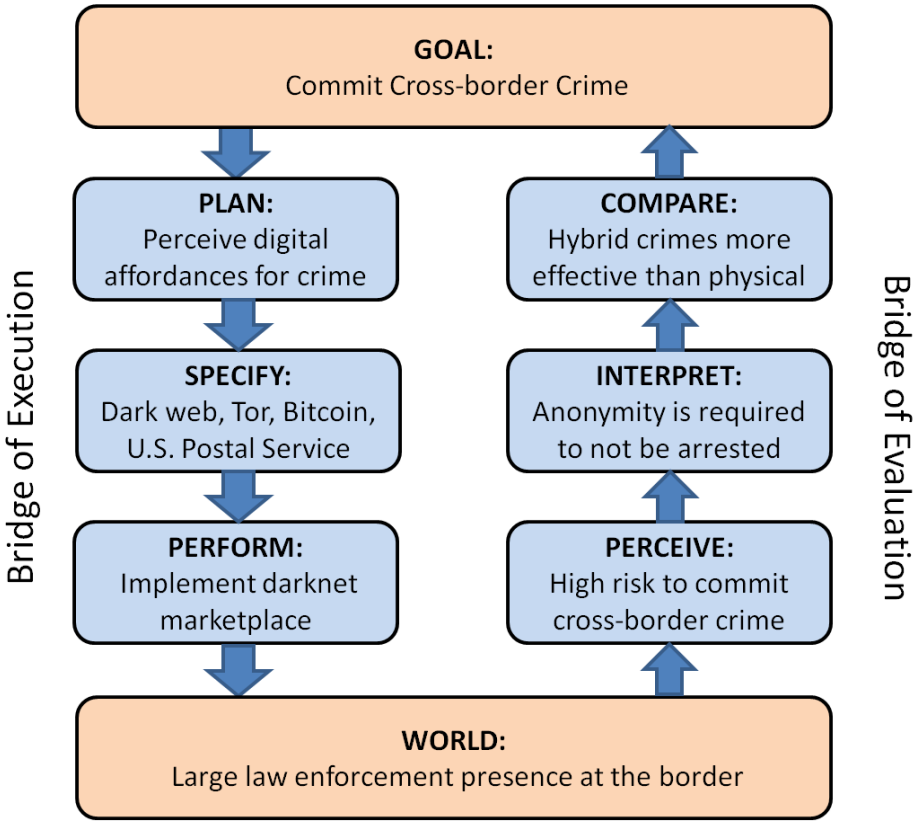

Figure 3. Adapted Model of Criminal Actions for Cross-border Crime[110]

[109] These actions are explained more in Chapter IV.

[110] Adapted from Norman, *The Design of Everyday Things*, 40–46.

3. Constraints

Constraints are an important component to consider when determining action possibilities of any object, whether digital or physical. Norman identifies four constraints that limit action and the perception of affordances: physical, cultural, semantic, and logical.[111] An example of a physical constraint for a hybrid crime would be the inability to smuggle drugs physically across the border using the Internet. A cultural constraint could be a person's ethics. For example, an ethical person might not be able to mentally conceive a heinous criminal act. A semantic constraint limits actions based on past knowledge of norms.[112] At one time, for example, a carriage could not afford movement if it was horseless. That affordance constraint changed once automobiles—then referred to as horseless carriages—were invented. A logical constraint limits action possibility to logical, realistic responses.[113] For instance, if someone is putting a puzzle together and there is only one piece remaining, it is logical where the one puzzle piece must be placed.

In design theory, constraints guide product development, ensuring the products function properly and realistically, and in ways that are obvious to users.[114] Criminals may view constraints as an obstruction to overcome in order to commit crime. For the study of crime, constraints should be viewed as a tool to limit the scope of possible actions for a given object. Constraints can focus on perceiving technological affordances to determine possibilities for disrupting crime, rather than on more manageable criminal uses of technology. However, because action possibilities from Internet technologies are intangible, it is not so simple a feat to limit actions based on constraints.

For the purposes of this study, constraints can both simplify and complicate affordance theory analysis. If done properly, determining an object constraint can prevent wasted analysis for a technology that cannot perform a certain function. Inversely, an

---

111 Norman, *The Design of Everyday Things*, 125.

112 Ibid., 129–130.

113 Ibid., 130.

114 Ibid., 123–132.

improper constraint determination can lead to misperceptions about technologies' criminal uses and inadequate predictability.

The next chapter uses the Silk Road darknet marketplace as a case study to identify how technologies afforded unique ways to commit cross-border crime. The Silk Road was the first darknet marketplace of its kind and was the originator of large-scale hybrid crime. As shown in the case study, law enforcement had difficulty adapting to the changing criminal typology and used traditional enforcement techniques to counter hybrid challenges. The second case study, in Chapter V, looks at the Silk Road 2.0 and shows how law enforcement adapted techniques to better handle the challenges of hybrid crimes.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDY 1: THE SILK ROAD

> During the past fifteen years, technological innovation and globalization have proven to be an overwhelming force for good. However, transnational criminal organizations have taken advantage of our increasingly interconnected world to expand their illicit enterprises.
>
> —President Barack Obama[115]

This chapter reviews the Silk Road darknet marketplace to explain the challenges law enforcement faced when trying to stop illegal drug smuggling facilitated by the Internet. The first section of this chapter explains what the Silk Road is, who created it, and the technologies that afforded the creation of a new hybrid category of crime. As part of the explanation, the Silk Road's unique Internet technology uses are compared with normal uses, in an effort to identify affordances. The second section shows the investigative techniques law enforcement used to respond to the Internet's new technological uses. What is especially significant in this section is how law enforcement was able to use traditional investigative techniques to overcome the hybrid crime, despite its inability to overcome new criminal uses of Internet technology. This section highlights areas of vulnerability within hybrid crime and identifies a starting point in the stigmergic cycle that exists between criminals and law enforcement. The final section provides conclusions about affordances vis-à-vis law enforcement adaptability.

A. FOLLOW THE SILK ROAD: THE GENESIS OF HYBRID CRIME

The Silk Road was the first darknet marketplace of its kind and relied on unique Internet technologies to facilitate crime. Like its namesake, the 4,000-mile ancient trading route linking China to Rome, the Silk Road involved global commercial activity. However, unlike the ancient trading commodities of silk, wool, gold, and silver, the commodities of the Silk Road comprised illegal drugs, guns, stolen credit cards, fraudulent documents, computer viruses, child pornography, and murder for hire.[116] This

115 Andreas, *Smuggler Nation*, 331.

116 Goodman, *Future Crimes*, 245.

illicit marketplace created an easy pathway for criminals to commit crimes, sheltering them from prosecution and allowing them to profit from illicit gains. Ross William Ulbricht (also known as "Dread Pirate Roberts"), the sole creator of the Silk Road, understood the Internet's complexities as a system of systems and envisioned new, unique uses for its technologies.[117]

Ulbricht started to envisage the Silk Road sometime between 2008 and 2010 when he was approximately twenty-five years old.[118] His desire to create a darknet marketplace was precipitated by his libertarian belief in free markets, and his objection to government control of consumerism, to include the sale and purchase of illegal drugs.[119] Because he was not a narcotrafficker, career criminal, or serious drug user, Ulbricht did not fit the typical criminal profile. Moreover, without computer science credentials or past work as a programmer, he seemingly lacked the technical ability to create a significant darknet market. A bachelor's degree in physics and a master's degree in science and engineering, however, may have trained him to perceive affordances more creatively than the average criminal.[120]

The path Ulbricht took to perceive and conceive a darknet criminal marketplace is critical to this study. His ability to map unintended signifiers led him to recognize—before anyone else—a set of yet unrealized action–object relationships, or affordances, for Internet technologies. A signifier is a perception or sign of an object's potential.[121] Signifiers go hand-in-hand with affordances; in the normative context of design theory, a signifier must be readily apparent to build user-friendly products.[122] Unlike in design theory, however, unintended signifiers in the context of Internet-facilitated crime are not obvious or apparent unless the technology is designed specifically for the purpose of criminal activity.

---

117 Goodman, *Future Crimes*, 245–249.

118 Bilton, *American Kingpin*, 33.

119 Ibid., 20, 22, 34.

120 Ibid., 14; Goodman, *Future Crimes*, 249.

121 Norman, *The Design of Everyday Things*, 13–19.

122 Ibid.

The first affordance Ulbricht perceived was the Internet itself. Though Ulbricht was not the first to recognize that the Internet afforded criminal activity, he pioneered its use to convert purely physical smuggling into a digital–physical hybrid crime. The new hybrid category maintained both physical and digital components; rather than constraining the Internet to its intended uses (e.g., sharing research and facilitating social connectivity), Ulbricht identified unintended signifiers that facilitated border-related crime.

While the *possibility* to intermix elements of physical crimes and cybercrimes was not new, it had never been accomplished as successfully as in the Silk Road. In the past, smuggling was achieved by the illegal physical movement of people or goods in and out of the United States—a person had to physically smuggle a commodity and receive illicit payment, making it a traditionally physical crime. In the more recent past, smuggling also became digital for certain commodities, such as intellectual property and child pornography. Those specific commodities could have remained digital forever, resulting in purely traditional cybercrimes. Using the Internet, however, Ulbricht intertwined purely physical smuggling into an interdependent relationship with the digital realm.

Ulbricht realized the Surface Web could not completely serve his needs; although it afforded the global connectivity and communications needed for a marketplace, it did not afford anonymity. In search of anonymity, Ulbricht's mapping of Internet affordances led him to the deep web, which is intended for large data storage.[123] He perceived the deep web's secrecy as a means for concealing illegal activity, his own identity, and the identities of drug vendors and buyers. Using the deep web as a platform, Ulbricht could make the Internet a central feature of smuggling while retaining anonymity. The sector of the deep web that afforded Ulbricht this capability, along with global connectivity and communications, was the dark web.

Ulbricht next began to seek Internet technologies that would afford criminal advantages, the most valuable of which was Tor. Originally developed to allow the U.S. military to securely communicate with foreign military intelligence and overseas assets,

123 Bilton, *American Kingpin*, 34.

Ulbricht first learned about Tor in online chat rooms as early as 2009.[124] Despite Tor's known affordance, Ulbricht was constrained neither by its intended action properties nor by the lack of new ideas; he recognized signifiers that Tor could be used to facilitate hybrid crimes—namely, the security and anonymity required to create a darknet marketplace.

At this point, Ulbricht had identified all the technologies needed to build a darknet marketplace; the only missing piece was the ability to receive anonymous payments for illegally smuggled goods.[125] A market of this kind could not rely on traditional financial institutions or cash payments because of the continuing necessity to remain anonymous and the large volume of transactions. This part of the crime had to remain digital. Ulbricht realized he could only act on his plan if there was a way to anonymize online payment transactions.[126] In 2010, he discovered that Bitcoin and Bitcoin tumbler could fulfill these missing affordances.[127] Bitcoin was developed to decentralize online payments outside of the banking system.[128] Bitcoin payments are pseudo-anonymous, and a Bitcoin payment system can be built into a darknet marketplace itself. Ulbricht wrote thousands of lines of code to connect Bitcoin to the other components of his hidden website.[129] He relied on a Bitcoin tumbler to further anonymize the online payments by mixing multiple transactions, making them harder to trace.

Ulbricht had mapped out all the technological pieces for creating a darknet marketplace, and he was confident law enforcement could not counter the anonymity afforded by the technologies. He changed the rules of crime and crime enforcement when he made the online marketplace viable for smuggling illegal goods. Ulbricht's unique ability to recognize affordances and unintended signifiers meant he had an advantage over law enforcement, which had not yet perceived the same action possibilities for the

---

124 Stone and Poladian, "Meet the Deep Web; Bilton, *American Kingpin*, 34

125 Bilton, *American Kingpin*, 34–35.

126 Ibid., 35

127 Ibid.

128 Elwell, Murphy, and Seitzinger, *Bitcoin*, 3.

129 Bilton, *American Kingpin*, 43–44.

dark web, Tor, Bitcoin or Bitcoin tumbler. In creating the Silk Road, Ulbricht had taken away much of the effectiveness of traditional border enforcement and investigative techniques. There were no longer individuals who could be surveilled on street corners, where they met to make drug transactions: the meeting would happen in the dark web. Drug "mules," who could be apprehended and "turned" to cooperate with authorities, would no longer be bringing illegal drugs across the border; illegal drugs would be shipped directly to consumers through the U.S. Postal Service. Illicit cash payments or wire transfers could no longer be analyzed to identify suspects; payments would now be made by Bitcoin. Ulbricht's creation of a hybrid crime was effective at stymying law enforcement efforts.

In January 2011, Ulbricht launched the Silk Road under the URL tydgccykixpbu6uz.onion, and later silkroadvb5piz3r.onion.[130] Relying on the anonymity afforded by the new Internet technologies, Ulbricht thought he would not get caught. The modern Silk Road was in business from approximately January 2011 to September 2013 before the website was seized and the creator arrested in San Francisco, California, by U.S. law enforcement.[131] In its two and a half years of operation, the Silk Road had approximately 957,000 registered user accounts, earned $1.2 billion in overall revenue, and profited $80 million in commission.[132] Figure 4 shows a screenshot of what the Silk Road website looked like and the variety of illegal goods for sale.

[130] Bilton, *American Kingpin*, 44; United States of America v. Ross William Ulbricht, Sealed Complaint, Southern District of New York, 1:13-cb-06919-KBF, October 2, 2013, 9.

[131] United States v. Ross William Ulbricht, Sealed Complaint, 2.

[132] Ibid., 6.

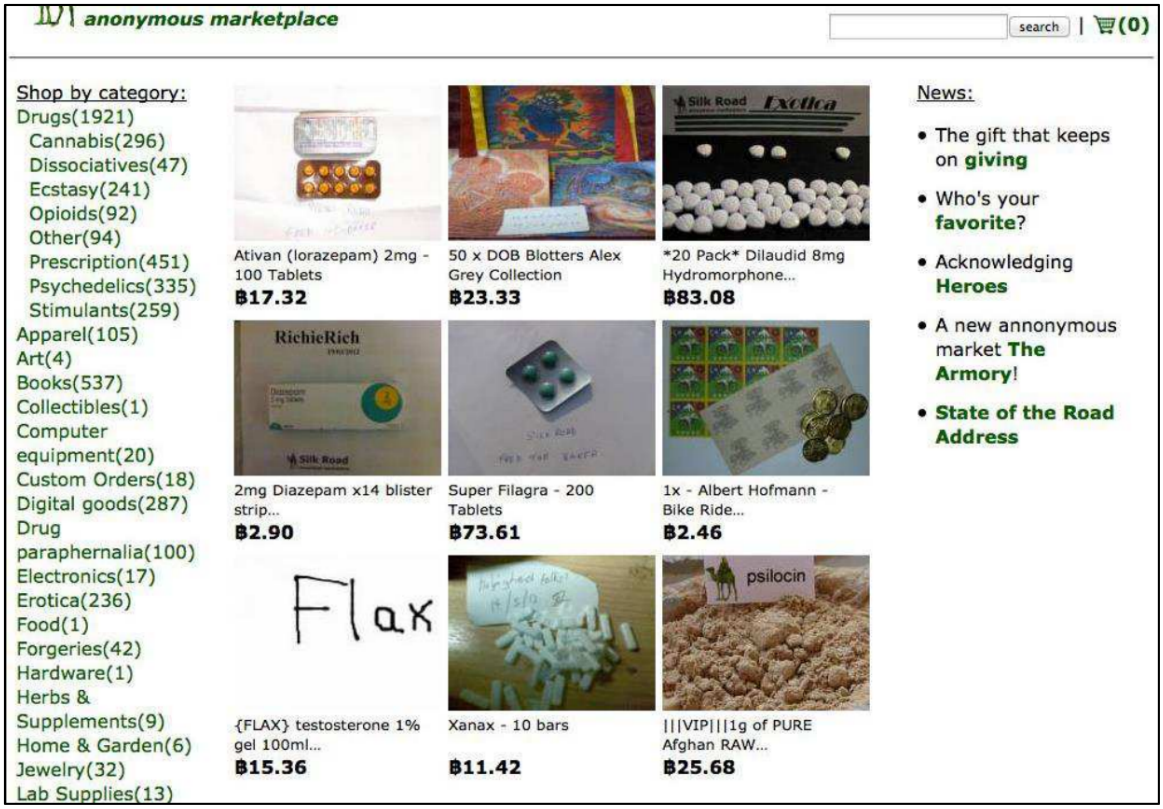

Figure 4. Screenshot of the Silk Road Website[133]

Although Ulbricht was identified and arrested, there is no direct evidence that law enforcement was able to overcome the technology affordances he used to smuggle illegal goods. Ulbricht's perceived signifiers and their technology affordances were accurate, and the crimes' digital components performed well—Tor, Bitcoin, and Bitcoin tumbler maintained the vendors' and buyers' anonymity. The physical component of the crime also performed well—illegal drugs were successfully smuggled into the United States through the U.S. Postal Service, and only a small percentage of packages were seized through law enforcement interdiction efforts. Ulbricht's perceived criminal Internet affordances, the product of his natural mapping, were sound. Fortunately for law enforcement, Ulbricht left a digital shadow in the Surface Web that allowed traditional

133 Source: David Décary-Hétu and Luca Giommoni, "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous," *Crime, Law and Social Change* 67, no. 1 (2017): 59.

investigative techniques to overcome his anonymity. The following section explains how law enforcement adapted to the challenges presented by the Silk Road.

B. LAW ENFORCEMENT RESPONDS USING OLD METHODS

This section summarizes how law enforcement investigated the Silk Road, explains how the Internet affordances on which Ulbricht relied impacted enforcement, and describes how law enforcement countered the affordances. While the Silk Road case study shows Ulbricht's superior ability to recognize signifiers of Internet affordances, it also shows law enforcement's perseverance to stop crime. Specifically, it shows how law enforcement adapted traditional investigative techniques to be effective against the new hybrid crime of border smuggling.

The Silk Road investigation was a priority for many agencies and government officials. The main law enforcement agencies involved in the investigation included Immigration and Customs Enforcement's Homeland Security Investigations (HSI), Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), U.S. Secret Service, U.S. Postal Inspection Service, U.S. Customs and Border Protection (CBP), and Internal Revenue Service (IRS).[134] Having so many agencies involved in the criminal investigation provided significant leverage of skills and authorities, but it did not prove helpful for resolving the case quickly. Law enforcement recognized the hybrid nature of the darknet marketplace, yet relied on traditional criminal and established cybercrime investigative techniques to overcome the Internet technologies' anonymity affordances. Law enforcement did not devise new, smart hybrid investigative methods or directly perceive Internet affordances to counter the new smuggling technique.

The CBP and HSI began investigating the Silk Road in October 2011, and realized that small personal-use quantities of drugs seized at the foreign mail unit in Chicago showed relational patterns.[135] The CBP and HSI made thousands of drug

134 "HSI Seizes Biggest Anonymous Drug Black Market Website and Assists in Arrest of Operator and Overseas Co-conspirators," ICE, accessed May 07, 2017, https://www.ice.gov/news/releases/hsi-seizes-biggest-anonymous-drug-black-market-website-and-assists-arrest-operator-and.

135 Bilton, *American Kingpin*, 3–9.

seizures through normal inspection efforts.[136] Because the drug sources were both international and domestic, agents were able to categorize packages into groups based on how labels were completed, as well as the packages' destinations and origins. These relational patterns helped identify the Silk Road's level of activity through recognized similarities (for instance, the packages were shipped through the U.S. Postal Service) and allowed law enforcement to follow up with knock and talks—a technique in which officers visit an address of interest, knock on the door, and interview a person who might have information about specific criminal activity.[137] When HSI conducted knock and talks at addresses listed on seized packages, they were able to identify the connecting factor: the Silk Road.[138] These inspection and interdiction efforts—physical seizures, knock and talks, and interviews—are all traditional investigative techniques that successfully gathered evidence about the Silk Road, but they were not able to identify Ulbricht.

Using an undercover technique, the HSI and DEA set up new Silk Road accounts, and took over existing accounts of users who were cooperating with the government.[139] Through these undercover accounts law enforcement gathered evidence of drug smuggling, communicated directly with Ulbricht, and even made online undercover purchases.[140] This is an established, traditional technique frequently used to investigate cybercrimes; although it also enabled law enforcement to successfully gather evidence, it again was not able to identify Ulbricht. Although the HSI and DEA both had undercover communications directly with Ulbricht's anonymous Internet pseudonym, Ulbricht's understanding of Internet technologies' anonymity affordances protected his identity and his computer's IP address.

---

136 Bilton, *American Kingpin*, 150.

137 Bilton, *American Kingpin*, 5.

138 Ibid., 6–7.

139 Ibid., 83–85, 100–102, 239–241; United States v. Ross William Ulbricht, Sealed Complaint, 11.

140 Bilton, *American Kingpin*, 83–85, 100–102, 239–241; United States v. Ross William Ulbricht, Sealed Complaint, 11.

The FBI was the first to devise a method to identify Ulbricht when investigators discovered a vulnerability in a script written to update the Silk Road website's login page.[141] The vulnerability allowed the FBI to identify the IP address of a Silk Road server housed in Iceland; they seized an imaged copy and replicated the server, after which they were able to gather vast amounts of information about the Silk Road's communication flow and inner workings—including individual communications, transactions, and Bitcoin exchanges—as well as evidence pointing to Ulbricht as the site's owner and operator.[142]

Seizing servers is a common technique used in cybercrime investigations. Even with the server, however, the FBI was still unable to counter Ulbricht's Internet anonymity affordance. The one piece of information about the server that was crucial to eventually unraveling Ulbricht's anonymity was the name of the server, Frosty.[143] Eventually, using traditional investigative techniques, law enforcement was able to link the server's name to Ulbricht's computer, which was also named Frosty.[144]

The IRS was the first to crack Ulbricht's anonymity, but did so using traditional law enforcement techniques (analysis and subpoenas) rather than by identifying signifiers for new technology to counter Tor's anonymity affordances. The IRS searched the Surface Web for the very first mention of the Silk Road and found a magic mushroom forum called Shroomery, as well as a second mention on a Bitcoin forum called Bitcointalk.[145] Both posts were linked to the same user name, which was later linked to another post that mentioned a Bitcoin start-up company and noted an email address.[146] When the IRS issued a subpoena to Google for the email address's subscriber information, Ulbricht was identified.[147] The IRS was then able to determine that

---

[141] Bilton, *American Kingpin*, 221–222.

[142] United States v. Ross William Ulbricht, Sealed Complaint, 14–24;. Bilton, *American Kingpin*, 14–15, 221–223.

[143] United States v. Ross William Ulbricht, Sealed Complaint, 32.

[144] Bilton, *American Kingpin*, 268.

[145] United States v. Ross William Ulbricht, Sealed Complaint, 24–26.

[146] Ibid., 26.

[147] Ibid.

Ulbricht's personal email and a computer connected to the seized Silk Road server were located in geographic proximity to one another, in San Francisco.[148]

Another direct correlation between Ulbricht and the Silk Road came from Ulbricht himself. In an unrelated enforcement action, CBP intercepted a package from Canada, shipped to Ulbricht, containing nine counterfeit identity documents.[149] The documents were replications of legitimate documents from various states that had different names but the same photograph.[150] When HSI visited the address on the receiving end of the package, they encountered Ulbricht and realized that he matched the photograph on the documents.[151] When questioned by agents, Ulbricht mentioned that, "hypothetically," people could buy counterfeit identity documents from the Silk Road using Tor.[152]

Ulbricht was not arrested for purchasing the fraudulent identity documents, and HSI did not immediately understand the significance of the Silk Road. However, when the IRS searched HSI's case management system and found this interaction, it was the first piece of evidence directly linking Ulbricht to the Silk Road.[153] The IRS also located an online post in which a person named Ross Ulbricht posed questions about coding and Tor.[154] The important part of the discovery was that the username on the forum was changed from "Ross Ulbricht" to "Frosty."[155] The FBI immediately recognized the connection to the name of the seized server and the computer owned by the Silk Road's operator.[156]

---

148 United States v. Ross William Ulbricht, Sealed Complaint, 27–28.

149 Bilton, *American Kingpin*, 264–265.

150 Ibid.

151 United States v. Ross William Ulbricht, Sealed Complaint, 28–29.

152 Ibid.

153 Bilton, *American Kingpin*, 264–265.

154 Ibid., 267–268.

155 Ibid., 268.

156 Ibid.

On October 1, 2013, Ulbricht was arrested in a San Francisco library; the anonymity he worked so hard to achieve and build into the Silk Road had been breached.[157] He was extradited to the Southern District of New York where he was eventually placed on trial and found guilty of aiding and abetting the distribution of drugs, continuing a criminal enterprise, computer hacking conspiracy, fraud with identification documents, and money laundering conspiracy.[158] On May 29, 2015, Ulbricht was sentenced to life imprisonment and ordered to forfeit $183,961,921.[159]

C. SILK ROAD CONCLUSIONS: AFFORDANCES ALMOST WIN

The Internet affordances Ulbricht found in the dark web, Tor, Bitcoin, and Bitcoin tumbler worked perfectly to achieve anonymity. Because of the technologies, Ulbricht was able to achieve his goal of creating a darknet marketplace. The Achilles heel in Ulbricht's plan was the vulnerabilities in transitioning drug smuggling from a purely physical crime to a hybrid crime. Ulbricht's downfall was in this transition.

Because his darknet marketplace was hidden even from the digital world, Ulbricht had to find a way to alert potential customers to its existence. To do so, he attempted to discreetly market the Silk Road on Surface Web forums.[160] This marketing attempt left a trail for law enforcement to follow. Ulbricht also sought to personally obtain fraudulent identity documents through the Silk Road, a hybrid border-related crime of its own. When the fraudulent documents were interdicted and he mentioned the Silk Road "hypothetically" to HSI agents, the clue was eventually enough to link Ulbricht to the

---

157 Natasha Bertrand, "The FBI Staged a Lovers' Fight to Catch the Kingpin of the Web's Biggest Illegal Drug Marketplace," *Business Insider*, May 29, 2015, http://www.businessinsider.com/ross-ulbricht-will-be-sentenced-soon--heres-how-he-was-arrested-2015-5.

158 United States v. Ross William Ulbricht, Judgement in a Criminal Case, 1:14-cr-00068-KBF (SD NY, May 29, 2015); Controlled Substances—Possession with Intent, 21 U.S.C. § 848(a) (2009); Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030(b) (2011); Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and information, 18 U.S.C. § 1028(f); Laundering of Monetary Instruments, 18 U.S.C.§ 1956–4999(F).

159 United States v. Ross William Ulbricht, Judgement in a Criminal Case.

160 United States v. Ross William Ulbricht, Sealed Complaint, 24–26.

marketplace. Finally, a website maintenance programming mistake—a purely digital component of the crime—helped law enforcement identify Ulbricht's server.[161]

As mentioned, law enforcement relied on traditional investigative techniques, including knock and talks, undercover activity, targeted interdictions, seizures, forensic analysis of electronic evidence, and analysis of open-source material. In defense of its ability to anonymize users, the Tor Project released a statement about Ulbricht's arrest, explaining that only traditional law enforcement methods were used to identify and arrest Ulbricht. The Tor Project stated, "[Ulbricht] 'made mistakes in operational security' and was caught by 'actual detective work' rather than exploiting problems with Tor."[162] This research, too, could not find evidence that law enforcement relied on anything other than traditional investigative techniques.

Ulbricht perceived using the Internet for an anonymous, free-market criminal enterprise; while Internet technologies were fully capable of communicating information anonymously between drug distributors and buyers, the Internet did not initially have the technology to anonymously transfer funds for drug transactions. Ulbricht's creation of the Silk Road was stopped dead in its tracks until he learned of Bitcoin. Bitcoin, a virtual currency, can be considered disruptive technology; it was new, and it served as the final puzzle piece that allowed Ulbricht to create a darknet marketplace. While the Silk Road investigation demonstrates how Ulbricht perceived a signifier (developing a free market criminal enterprise) and how Bitcoin ultimately facilitated the affordance's final realization, it does not demonstrate law enforcement's ability to develop new affordances.

The Silk Road investigation is the best documented example of a large-scale darknet marketplace used to implement Internet affordances that created hybrid crimes. Although law enforcement did successfully identify and arrest Ulbricht, and seize the Silk Road website, there is no indication that law enforcement was able to directly overcome Ulbricht's Internet affordances. The dark web, Tor, Bitcoin, and Bitcoin

---

[161] Bilton, *American Kingpin*, 221–222.

[162] Chloe Albanesius, "What Was Silk Road and How Did it Work?" *PCMAG,* October 3, 2013, http://www.pcmag.com/article2/0,2817,2425184,00.asp.

tumbler all performed as Ulbricht had perceived to maintain anonymity. Instead, law enforcement was able to indirectly overcome Ulbricht's Internet affordances by relying on traditional law enforcement and established cybercrime techniques that capitalized on the vulnerabilities created when Ulbricht converted a purely physical crime into a hybrid crime.

Because law enforcement was not able to directly overcome the technologies, not even Ulbricht's arrest, conviction, and life sentencing were enough to deter or prevent additional illicit entrepreneurs from creating darknet criminal marketplaces. Enforcement displaced criminals from the seized Silk Road, but darknet criminal marketplaces still began to thrive, and the digital elements of the hybrid crime were not displaced from the Internet back into the physical world. In other words, the seizure of the Silk Road simply displaced the criminal activity to a new digital street corner in the Dark Web; it did not produce a crime-free neighborhood. Silk Road 2.0 was one of the darknet criminal marketplaces created after the demise of the Silk Road. The following chapter explains Silk Road 2.0 and discusses law enforcement adaptability.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY 2: OPERATION ONYMOUS—CRIMINAL AFFORDANCE ANALYSIS FOR NARCOTRAFFICKING

> Underground websites such as Silk Road and Silk Road 2 are like the Wild West of the Internet, where criminals can anonymously buy and sell all things illegal.
>
> —Peter Edge, Executive Associate Director, HSI[163]

Operation Onymous was a multi-agency global operation that began on November 5, 2014, to respond to a large number of darknet marketplaces created after the seizure of the Silk Road.[164] Silk Road 2.0 was one of the marketplaces that law enforcement seized during the operation.[165] This chapter reviews Silk Road 2.0 to explain the challenges law enforcement faced when trying to stop illegal drug smuggling facilitated by the Internet. The first section describes Silk Road 2.0 and its creators, and briefly discusses the technologies that afforded the new hybrid crime category. As part of the discussion, this section explains the continuing stigmergic cycle between criminals and law enforcement through the creation of numerous darknet marketplaces identified during Operation Onymous. The second section shows how law enforcement learned to adapt to hybrid crime and overcame anonymity afforded by Tor. It shows how law enforcement found a vulnerability in the technology and was able to manipulate Tor's normal action–object relationship. This adaptably is important; it shows that law enforcement stopped relying solely on traditional techniques and devised new means of overcoming criminal uses of Internet technology to counter hybrid crime. The final section provides conclusions about affordances vis-à-vis law enforcement adaptability.

---

163 "Dozens of Online 'Dark Markets' Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0," United States Department of Justice, November 07, 2014, https://www.justice.gov/usao-sdny/pr/dozens-online-dark-markets-seized-pursuant-forfeiture-complaint-filed-manhattan-federal.

164 Décary-Hétu and Giommoni, "Police Crackdowns."

165 Department of Justice, "Dark Markets."

A. HYBRID CRIMES GO MAINSTREAM: OPERATION ONYMOUS AND SILK ROAD 2.0

After the Silk Road was seized and Ulbricht arrested, Internet anonymity affordances became public knowledge. As a consequence, the prospect of committing hybrid crime became more inviting and creation of darknet marketplaces skyrocketed. This section describes how law enforcement responded to this surge of new darknet marketplaces, focusing particularly on Silk Road 2.0. The response included a global law enforcement operation called Operation Onymous.

Operation Onymous involved the Department of Justice, FBI, HSI, DEA, and law enforcement from at least sixteen foreign countries.[166] The operation's results were staggering: they included seventeen arrests, $1.3 million in seized Bitcoins, and twenty-seven darknet marketplace seizures.[167] Before they were seized, these marketplaces facilitated various hybrid crimes including the sale of "illegal narcotics, firearms, stolen credit card data and personal identification information, counterfeit currency, fake passports and other identification documents, and computer-hacking tools and services."[168] Marketplaces that were seized as a result of the operation included: Alpaca; Black Market; Blue Sky; Bungee 54; Cabbabis UK; Cloud 9; Dedope; Farmer1; Hydra; Pablo Escobar Drugstore; Pandora-Pandora; Smokeables; Tor Bazaar; Fake Real Plastic; Pandora; Pay Pal Center; Real Cards Team-Team; The Green Machine; Zero Squad; Alpaca, Blue Sky; Fast Cash!; Sol's Unified USD Counterfeit's; Super Note Counter; The Hidden Market; Fake ID; Pandora, Silk Road 2.0; and Silk Road 2.0.[169] While all these seizures were important, the Silk Road 2.0 provides the best comparisons relative to the original Silk Road.

---

166 Department of Justice, "Dark Markets."

167 Décary-Hétu and Giommoni, "Police Crackdowns"; Kate Vinton, "So Far Feds Have Only Confirmed Seizing 27 'Dark Market' Sites in Operation Onymous," *Forbes*, November 09, 2014, https://www.forbes.com/sites/katevinton/2014/11/07/operation-onymous-dark-markets/#246db0672fcf.

168 Department of Justice, "Dark Markets."

169 Vinton, "Operation Onymous." Several copycat darknet marketplaces borrowed names from previously or currently popular marketplaces to attract recognition.

Silk Road 2.0 was created just five weeks after the original Silk Road was seized. It came to life with a new operator and new URL, http://silkroad6ownowfk.onion, but with the same goal of committing cross-border hybrid crime.[170] Silk Road 2.0 took over the role of facilitating the sale of such items as illegal drugs, fake passports, fake driver's licenses, website hacking services, and email hacking tools.[171] The same Internet affordances Ulbricht perceived—including anonymous communications and transactions through Tor, Bitcoin, and Bitcoin tumbler—were employed once again.[172] However, Silk Road 2.0 placed a strong emphasis on protecting its website servers' anonymity, presumably based on the belief that Ulbricht was identified through forensic analysis of a server. The original Silk Road 2.0 operator, known as Dread Pirate Roberts 2 (DPR2), announced in a forum to site vendors that "he had 'taken steps the previous Dread Pirate Roberts wouldn't have even thought of' to protect the servers that would run the new website."[173] DPR2 was never identified, but the new mindset of server protection carried forward to the next operator of the Silk Road 2.0.

Around November 2013, shortly after Silk Road 2.0 was created, Blake Benthall (known online as "Defcon"), replaced DPR2 as the site operator.[174] Benthall was twenty-six years old, originally from Houston, Texas, and reportedly grew up in a conservative Christian household.[175] He went to a Christian college called Florida College in Temple Terrace, Florida.[176] Benthall moved to San Francisco, California, where he worked as a software developer and programmer for RPX, Carbon Five, and SpaceX, and provided

170 *United States v. Blake Benthall*, Sealed Complaint, 8.

171 Ibid., 11–12.

172 Ibid., 9–11.

173 Ibid., 13.

174 Ibid., 14–15.

175 Rob Price, "How Friends saw Blake Benthall, the Accused Silk Road 2.0 Kingpin," *Daily Dot*, February 24, 2017, https://www.dailydot.com/crime/blake-benthall-silk-road-2-friends-coworkers-christian-bitcoin/.

176 Ibid.

freelance consulting to a startup company called Close.[177] Similar to Ulbricht, Benthall's libertarian ideals directed his actions to support an open market and the use of Bitcoin.[178] Ulbricht and Benthall appeared to have very similar backgrounds, social networks, and ideals that may have allowed them to perceive divergent, and illegal, Internet technology uses.

Like Ulbricht and DPR2, Benthall showed a desire to maintain and improve the Internet technologies that afforded him anonymity. Benthall seemed to focus the most concern, like DPR2, on website server vulnerabilities rather than on problems with Tor, Bitcoin, or Bitcoin tumbler technologies. In one forum post about the Silk Road 2.0 Bitcoin payment system, Benthall announced that Silk Road 2.0 had "increased server anonymity."[179] In another post he stated he was working "to expand our Bitcoin infrastructure's ability to process more cash deposits per minute while preserving server anonymity and security."[180] Benthall also posted a message to site administrators about protection of Silk Road 2.0 servers, stating, "Prevent[ing] servers from being seized by [law enforcement] … this has been consuming most of my time and I cannot elaborate on it, nothing's in danger, but scaling a site this large requires a lot of odd approaches to server stealth."[181] It is apparent that Benthall believed law enforcement had identified Ulbricht based on weaknesses in anonymity afforded to website servers, and he was working to avoid the same fate.

Another incident that contributed to Benthall's concern about website server anonymity occurred on July 30, 2014, as a result of a Tor Project public blog post. The Tor Project announced it had identified a group of relays that were placed within the Tor

177 Price, "How Friends saw Blake Benthall"; Robert McMillan, "Alleged Silk Road 2 Mastermind Worked for Ex-Googler's Secret Startup," *Wired*, November 10, 2014, https://www.wired.com/2014/11/alleged-silk-road-2-mastermind-worked-ex-googlers-secret-startup/.

178 Price, "How Friends saw Blake Benthall."

179 United States v. Blake Benthall, Sealed Complaint, 15.

180 Ibid.

181 Ibid., 20.

network for purposes of committing traffic confirmation and Sybil attacks.[182] A traffic confirmation attack is used to determine if relays are on the same circuit, and a Sybil attack is a way to subvert communication flows in a peer-to-peer network by manipulating the assumed identities of relays.[183] The relays causing the attacks were active within the Tor network from January 30, 2014, to July 4, 2014, and the Tor Project believed the attacks were designed to de-anonymize users.[184] At the time the Tor Project made the announcement, it was unknown who committed the attacks or why. In response to the blog post, Benthall posted, "We are confident our unordinary servers are relatively safer than most hosting approaches, but will be moving servers again today. … We are provisioning the replacements and not connecting to possibly compromised devices."[185] This network compromise was the first sign that Tor, as a technology, might not be able to afford the level of anonymity perceived by Ulbricht.

Despite the possible Tor vulnerabilities, Benthall successfully operated the Silk Road 2.0 marketplace and used its technologies to commit the hybrid crime of smuggling from November 2013 to October 2014.[186] The site offered 14,024 illegal drug sale listings, including heroin, cocaine, psychedelics, ecstasy, cannabis, and opioids.[187] There were also fake passports, driver's licenses, website hacking services, and email hacking offered for sale.[188] The marketplace generated $8 million in illicit sales each month by internationally linking thousands of unlawful vendors with over a hundred thousand buyers.[189] Territorial borders did not dissuade the smuggling, and the Internet affordances perceived by Ulbricht supported Benthall's objectives. However, Benthall's

182 "Tor Security Advisory: 'Relay early' Traffic Confirmation Attack," *Tor Blog*, July 30, 2014, https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack.

183 "Tor Security Advisory"; John R. Douceur, "The Sybil Attack," Microsoft, accessed November 18, 2017, https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf.

184 "Tor Security Advisory."

185 United States v. Blake Benthall, Sealed Complaint, 15–16.

186 Ibid., 1.

187 Ibid., 11–12.

188 Ibid., 12.

189 Ibid., 6–7.

objectives were not the only ones at work: the stigmergic cycle had swayed, and law enforcement was attempting to gain an advantage over the technological innovations, seeking new ways to identify and stop darknet marketplaces.

Even with Internet technologies affording anonymity, and the extra precautions to conceal servers, Benthall could not stop law enforcement from gathering evidence of criminal activity. Like the Silk Road investigation, law enforcement was able, again, to successfully gather evidence of criminal activity using traditional undercover and forensic analysis techniques. HSI had an undercover agent develop support staff access to the Silk Road 2.0 website in order to communicate directly with Benthall.[190] The agent was able to monitor Silk Road 2.0 website activity and compare it with communications received directly from Benthall. Additionally, the DEA conducted multiple undercover drug purchases online through the marketplace.[191] Advancing the investigation beyond gathering evidence, the FBI located and imaged a Silk Road 2.0 server found in a foreign country.[192] Once the server was identified, law enforcement sought information from the service provider; the service provider produced the email address blake@benthall.net, which helped identify Benthall as the Silk Road 2.0's operator.[193] The FBI was able to identify multiple service alerts sent directly to the email address, which further linked Benthall to the Silk Road 2.0 server.[194] To strengthen the connection, relevant IP address activity for the specific email address was linked to Benthall's physical locations at known times.[195]

The cooperative investigative efforts by FBI, HSI, and DEA developed enough probable cause to identify Benthall as the Silk Road 2.0 operator and issue a federal warrant for his arrest. U.S. law enforcement authorities arrested Benthall on November 5, 2014, in San Francisco; he was charged with conspiracy to commit narcotics trafficking,

190 United States v. Blake Benthall, Sealed Complaint, 6.

191 Ibid., 12.

192 Ibid., 21.

193 Ibid., 23.

194 Ibid.

195 Ibid., 24–25.

aiding and abetting computer hacking, transferring fraudulent identification documents, and money laundering.[196] He was brought to the Southern District of New York to face the criminal charges. In addition to Benthall's arrest, the Silk Road 2.0 website was also seized. Benthall's case has been continued numerous times and is still pending a final disposition.

B. LAW ENFORCEMENT ADAPTABILITY FORCES ACTION–OBJECT RELATIONSHIP CHANGES

The Benthall investigation is significant because it disclosed the technology and affordance similarities between the Silk Road and Silk Road 2.0. Although new techniques were not disclosed, the investigation highlighted which traditional law enforcement techniques were successful. Another investigation of Silk Road 2.0 subordinate operator Brian Farrell (who went by the online pseudonym "DoctorClu"), provides insight into new techniques adopted by law enforcement. The following information about Farrell's arrest shows how the stigmergic cycle was moved by law enforcement perceiving technology affordances to counter hybrid crime.

Similar to the investigations surrounding Ulbricht and Benthall, law enforcement relied on traditional enforcement techniques such as undercover activity, search warrants, and forensic analysis of seized computer storage devices to identify and gather evidence against Farrell. Law enforcement discovered Farrell's identity and location in Bellevue, Washington, based on an IP address that linked Farrell to the Silk Road 2.0 website.[197] When agents located Farrell's address they approached Farrell and his roommate for consensual interviews.[198] As a result of the interviews, law enforcement verified Farrell and his roommate were aware of the Silk Road 2.0 website and that Farrell had advanced

[196] United States v. Blake Benthall, Sealed Complaint, 1–5; Attempt and Conspiracy, 21 U.S.C § 846 (2012); Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030(a)(2), 2 (2017); Conspiracy to Transfer Fraudulent Identification Documents, 18 U.S.C. § 1028(a)(2); Money Laundering Conspiracy, 18 U.S.C. § 1956(a)(1)(A)(i), 1956(a)(1)(B)(i).

[197] United States v Brian Richard Farrell, Complaint for Violation, 2:15-cr-00029-RAJ (WD WA, January 17, 2015), 5.

[198] Ibid., 5–6.

computer skills.[199] After gaining cooperation from the roommate, conducting a search warrant, and seizing drugs and money, law enforcement interviewed Farrell again.[200] During this interview, when law enforcement asked Farrell to identify people involved in the Silk Road 2.0, he replied, "You're not going to find much of a bigger fish than me ... My moniker on Silk Road was 'DoctorClu.'"[201]

While this exchange does not disclose anything new about technology or affordances, one matter disclosed in a search warrant affidavit eventually brought new investigative techniques to light: how law enforcement identified Farrell's IP address. In an affidavit written in support of establishing probable cause for a search warrant, an agent wrote that "an FBI 'source of information (SOI)' provided 'reliable IP addresses for TOR and hidden services such as SR2.'"[202] Additionally, the agent wrote, "The SOI also identified approximately 78 IP addresses that accessed a vendor .onion address," which led to Farrell's IP address.[203] Knowing that Farrell relied on Tor for anonymity, his defense counsel wanted to know how agents identified Farrell's IP address; the result was a back-and-forth legal struggle between the prosecution and defense about how much information should be disclosed regarding investigative techniques.

In response to discovery demands, the prosecution provided Farrell's defense counsel with a letter, which disclosed that Farrell was linked to Silk Road 2.0 "based on information obtained by a 'university-based research institute' that operated its own computers on the anonymous network used by Silk Road 2.0."[204] This information was released publicly in an order on defendant's motion to compel further discovery filed on February 23, 2016. Judge Richard A. Jones notes in the order that Farrell's "IP address was identified by the Software Engineering Institute (SEI) of Carnegie Mellon University

---

199 United States v Brian Richard Farrell, Complaint for Violation, 5–6.

200 Ibid., 6.

201 United States v Brian Richard Farrell, Complaint for Violation, 7.

202 Joseph Cox, "Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects," Motherboard, November 11, 2015, https://motherboard.vice.com/en_us/article/gv5x4q/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects.

203 Ibid.

204 Ibid.

(CMU) when SEI was conducting research on the Tor network which was funded by the [Department of Defense]."[205] As part of this research, SEI was reportedly "operating nodes" on the Tor network.[206] Judge Jones also disclosed the fact that the information about Farrell's IP address was obtained for the investigation "pursuant to a subpoena served on SEI-CMU."[207] Research shows that CMU SEI was deemed a federally funded research and development center (FFRDC) in 1984 to provide leadership and foster collaboration in the software and cyber communities.[208]

Although Judge Jones denied a motion to compel specific technical information about how law enforcement identified Farrell's IP address, and other government disclosures remain sealed, he required the prosecution to disclose general information about how the IP address was located. The court documents disclose that law enforcement, with help from CMU SEI, found a way to de-anonymize Tor.[209] This revelation rendered Tor—trusted by Ulbricht, Benthall, and Farrell—no longer trustworthy. This is a significant disclosure because it shows how law enforcement adapted to Tor's anonymity affordances and developed a method for manipulating its vulnerabilities. It also demonstrates how technically advanced the Internet has become: law enforcement had to seek outside expertise from CMU.

Judge Jones' order also reaffirmed a legal precedent relative to dark web privacy: although Tor is used for anonymity, its users' privacy is not legally protected.[210] Specifically, Judge Jones found that, because Tor users have no reasonable legal expectation of privacy, law enforcement did not conduct a true "search" when it relied on SEI to locate Farrell's IP address.[211] The judge stated, "In order for a prospective user to

---

205 United States v Brian Farrell, Order on Defendant's Motion to Compel, CR15-029RAJ (WD WA, February 23, 2016), 1–2.

206 United States v Brian Farrell, Order on Defendant's Motion to Compel, 1–3.

207 Ibid., 2.

208 "Why Work With an FFRDC," November 13, 2017, accessed November 19, 2017, http://www.sei.cmu.edu/about/organization/workingwithanFFRDC.cfm.

209 United States v Brian Farrell, Order on Defendant's Motion to Compel, 1–2.

210 Ibid., 2–3.

211 Ibid.

use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations. Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers."[212] The judge relied on the precedent from United States v. Forrester and United States v. Michaud to make his decision. In United States v. Forrester, the court found no expectation of privacy for IP addresses because they are "provided to and used by Internet service providers for the specific purpose of directing the routing of information."[213] In United States v Michaud, "the court held that the IP address was public information."[214] These findings created a legal precedent: that there are no privacy protections for people trying to anonymize themselves using Tor.

The Tor Project subsequently released a statement indicating that they believed SEI executed traffic confirmation and Sybil attacks on the Tor network to de-anonymize users.[215] The project identified a group of suspicious relays located in the network between January 30, 2014 and July 4, 2014.[216] A traffic confirmation attack occurs, the Tor Project explained, by a user controlling or observing entry and exit relays on both ends of a Tor circuit to compare traffic timing, volume, or other characteristics to determine which relays are on the same circuit.[217] An attacker would then be capable of matching up IP addresses identified from the entry relay with the location the IP address was accessing from the exit relay.[218] The end result is de-anonymized communications. A Sybil attack is a way to subvert communication flows in a peer-to-peer network by

212 United States v Brian Farrell, Order on Defendant's Motion to Compel, 3.

213 Ibid., 2–3.

214 Ibid., 3.

215 "Tor Security Advisory."

216 Noor Alsaedi, A. Sali Fazirulhisyam Hashim, and Fakhrul Rokhani, "Detecting Sybil Attacks in Clustered Wireless Sensor Networks based on Energy Trust System (ETS)," *Computer Communications* 110 (2017): 75–82.

217 "Tor Security Advisory."

218 Ibid.

manipulating the assumed identities of relays.[219] A malicious relay, or node, can illegitimately claim to have multiple identities by creating new identities or impersonating existing ones.[220] The Tor Project stated the SEI Sybil attack on the Tor network involved introducing 115 fast non-exit relays that acted as entry guards, routing a significant amount of Tor communications initially through those 115 relays.[221] This allowed the attacker to collect IP addresses and complete traffic confirmation analysis.

The Tor Project's assertions were never proven. It can logically be assumed that, because Farrell's arrest and the seizure of Silk Road 2.0 were part of Operation Onymous, information from CMU SEI contributed to other law enforcement successes. What is known, based on the order from Judge Jones, is that law enforcement relied on information received from CMU SEI to identify Farrell's IP address, even though his identity was anonymized by Tor, which led to his successful prosecution. On June 3, 2016, Farrell entered a plea agreement and was found guilty of conspiracy to distribute cocaine, heroin, and methamphetamine; he was sentenced to ninety-six months incarceration.[222]

C. CONCLUSIONS ABOUT SILK ROAD 2.0: AFFORDANCES LOSE

The Silk Road 2.0 case study shows how hybrid crimes became more established by criminals as the criminals, in turn, became more accustomed to the Internet technologies. Benthall and Farrell believed the same Internet affordances used for the Silk Road would protect their anonymity while operating Silk Road 2.0. As shown by Operation Onymous, numerous other criminal actors operating in the dark web maintained the same Internet affordances originally perceived by Ulbricht. A proliferation of darknet marketplaces demonstrated an increased reliance on the dark web, Tor, Bitcoin, and Bitcoin tumblers to commit crime.

---

219 Douceur, "The Sybil Attack."

220 Alsaedi, Hashim, and Rokhani, "Detecting Sybil Attacks."

221 "Tor Security Advisory."

222 United States v Brian Richard Farrell, Judgment in a Criminal Case, 2:15CR00029RAJ-001 (WD WA, June 3, 2016).

Of significance for this study is that, despite Benthall and Farrell having a basis to trust their Internet affordances, as Ulbricht did, law enforcement changed the game by overcoming Tor's afforded anonymity. After investigating the Silk Road, law enforcement started perceiving certain Internet affordances differently, and adapted to them; they also began to view hybrid crimes differently, and devised investigative techniques outside of traditional methods. In essence, law enforcement used adaptation to change an understood action–object relationship among Tor, anonymity, and hybrid crime.

Part of this adaptation was federal investigators' realization that Internet technologies had surpassed their knowledge, and were thus impeding their ability to investigate hybrid crimes. Agents also realized they had to broaden their approach to fight hybrid crimes by seeking technical expertise outside of the law enforcement realm.

VI. CASE STUDY ANALYSIS AND FINDINGS

> The Web as I envisaged it, we have not seen it yet. The future is still so much bigger than the past.
>
> —Sir Tim Berners-Lee, inventor of the World Wide Web[223]

The Silk Road and Silk Road 2.0 cases demonstrate the changing categories of border-related crime. Both case studies show crime's physical and digital elements and tangible results from Internet technologies' action–object relationships. This chapter provides an analysis of hybrid crime based on data obtained from the case studies. The first section explains which initial research hypotheses are validated, invalidated, or inconclusive. The second section presents eight findings extrapolated from the case studies that illuminate the challenges law enforcement faces when countering the illegal movement of people and goods facilitated by the Internet.

A. ANALYSIS: WHAT CAN BE LEARNED FROM THE SILK ROAD AND SILK ROAD 2.0?

This study gathered data about the Silk Road and Silk Road 2.0 by analyzing available literature. The content helped identify the changing categorization of border-crime based on criminals' increased reliance on Internet technologies. Part of the analysis involved examining how criminal actors traditionally commit border-related crimes, the investigative techniques law enforcement traditionally employ, how criminal actors use the Internet to commit criminal activity, how law enforcement identifies criminal activity facilitated by the Internet, what law enforcement can do to overcome the Internet's unique affordances for border-related crimes, and the effectiveness of investigative techniques that can be used to enforce these crimes. Data has been synthesized to determine validity of the hypotheses and findings.

223 "Tim Berners-Lee Quotes," AZ Quotes, accessed December 6, 2017, www.azquotes.com/author/8668-Tim_Berners_Lee?p=1.

I believed at the outset of this research that criminal actors and law enforcement would have different Internet affordances pertaining to border-related crime; that hypothesis has been validated. Even though affordances are always present, people perceive them differently depending on their unique frameworks and constraints. Ulbricht, Benthall, and Farrell perceived an anonymity affordance from Tor, Bitcoin, and Bitcoin tumbler technologies, which allowed them to successfully create and operate the Silk Road and Silk Road 2.0. These darknet marketplaces existed for years and facilitated the smuggling of enormous cumulative quantities of illegal drugs into the United States, generating millions of dollars of illicit proceeds from Bitcoin transactions. Because Ulbricht, Benthall, and Farrell were able to perceive and actionize these affordances before law enforcement fully understood the technologies, they had the advantage.

While the case studies show that criminals and law enforcement perceived and exploited different Internet affordances, they do not show a wide technology gap between the two groups, as I originally hypothesized. It took law enforcement approximately two years to investigate the Silk Road, arrest Ulbricht, and seize the website. During those two years, law enforcement successfully gathered evidence of Ulbricht's illegal activities using traditional law enforcement techniques. Law enforcement's stumbling block was its inability to identify Ulbricht as the website operator due to the anonymity affordances from Tor, Bitcoin, and Bitcoin tumbler. Despite this immediate ability to "overcome" Tor, law enforcement eventually recognized vulnerabilities in this evolving hybrid crime category and identified Ulbricht using traditional law enforcement techniques.

It took law enforcement approximately one year to investigate Silk Road 2.0; arrest Benthall, Farrell, and others; and seize the website. During that year, law enforcement gathered ample evidence to prosecute the operators, and assisted foreign law enforcement officials with the much larger Operation Onymous. It is not unusual for a large-scale federal criminal investigation to take a year or more to fully conclude. Significantly, during the period between investigations of the Silk Road and Silk Road 2.0, law enforcement learned how to counter Tor's anonymity affordance.

Law enforcement was able to evolve its understanding of Internet technologies, which suggests that there is not a large technological gap between criminals and law

enforcement; the differing Internet affordances are better explained by the stigmergic cycle. The data clearly show how criminals and law enforcement are constantly trying to gain an advantage over one another in the stigmergic cycle of law and order. However, it is still unknown if law enforcement is reacting to criminal technological advancements, or if criminals are reacting to strong law enforcement efforts (as illustrated by the chicken-or-egg dilemma described in Chapter III). Which group is leading the stigmergic cycle: law enforcement or criminals? The most accurate answer, according to the data analysis, is: both. The data clearly show a strong causal relationship between criminals and law enforcement; that relationship has caused both crime and investigative techniques to evolve and adapt. Such evolution created the hybrid category of border-related crime. The birth of the Silk Road and Silk Road 2.0, as well as law enforcement's capacity to de-anonymize Tor, show adaptation at work, but do not show a large technological gap.

This thesis also hypothesized that deterrence could not be achieved without narrowing the technological gap between law enforcement and criminals; this hypothesis was inconclusive. I predicted that if law enforcement relied on traditional investigative techniques, rather than realizing the same Internet affordances perceived by criminals, agents would not be able to achieve general deterrence of crime. The case studies show divergent results from traditional and non-traditional law enforcement techniques, but both ultimately resulted in specific deterrence through arrests and seizures. Although specific deterrence was achieved, the case study data do not reveal how different types of investigative efforts correlate to general deterrence. I discovered that law enforcement efforts created displacement from one darknet marketplace to another; however, general deterrence was not achieved from either conventional or unconventional investigative techniques.

B. ANALYSIS AND FINDINGS

Border-related crimes have traditionally been physical crimes. It is easy for most people to understand this type of drug trafficking: A narcotrafficker smuggles large quantities of drugs across a border into the United States. Once those drugs are in the

United States, they are divided into smaller amounts and distributed to different states, cities, and towns. Likewise, it is easy to understand how bulk cash is physically smuggled across the border in the reverse direction to pay the narcotrafficker. Save for telephone calls and some electronic money transfers, the traditional understanding of drug trafficking is physical. The case studies show how the evolution of drug trafficking from a physical to a hybrid crime has created unique challenges for law enforcement, including changing established understandings. The following section discusses my findings based on analysis of the case studies.

1. Categories Matter for Criminal Typologies

Law enforcement uses different techniques to investigate criminal activity facilitated by physical and digital objects—there are established techniques for investigating cybercrime, and established techniques for investigating physical crimes. Despite the crossover from physical to digital, each type of investigation remains mutually distinct. When criminal activity falls outside of known categories, like in the Silk Road investigation, difficulties arise. Although clear criminal labels are not always apparent, they are important. They form or substantiate opinions, and influence actions and reactions. Failing to recognize and properly label new categories of crime can lead to inefficient and ineffective investigative techniques.

The Silk Road investigation shows how essential it is for law enforcement to recognize changing criminal typology, and how difficult it can be to do so in dynamic environments. Even though law enforcement recognized a divergent criminal smuggling method, the activity was not uniquely labeled as "hybrid." Rather than bulk drugs being physically smuggled across the border, the Silk Road involved only personal-use quantities, sent through the U.S. Postal Service; this change distanced suppliers from the physical criminal activity, which made it more difficult for law enforcement to identify suppliers or to link all smuggling activity to one specific organization. The digital element of illicit payment—instead of physical cash or electronic transfers, the Silk Road used Bitcoins—also posed a difficulty, allowing the transactions to hide in the dark web. When law enforcement viewed this hybrid crime through a traditional lens, agents relied

on conventional investigative techniques that could not efficiently identify Ulbricht. When the Silk Road investigation concluded, however, law enforcement was able to get results from traditional techniques, essentially pounding a square peg into a round hole.

2. Analytical Frameworks Require Adaptability

Historically, criminal justice and criminology studies have relied heavily on sociological frameworks to understand deviant behavior. While sociological frameworks might be effective for analyzing deviance, they are not effective for advancing technical understanding of crime facilitated by the Internet. Sociological frameworks focus on macro-analyses to determine what causes deviance; analysis of this sort does little to explain hybrid crime or to predict how Internet technologies might afford future criminal activity.

The Silk Road and Silk Road 2.0 case studies further demonstrate that traditional sociological frameworks do not add value for law enforcement agents who are investigating hybrid crime. Ulbricht and Benthall both had similar libertarian ideals, but also conservative religious upbringings that do not match normal drug trafficking indicators. Even if Ulbricht and Benthall's behavior could be analyzed for factors that caused deviance, the resulting data would not help law enforcement create more effective enforcement strategies. A better practical approach for law enforcement purposes is to analyze how Internet technologies facilitated the border-related crime.

Rather than relying on physical actions, Ulbricht used Internet technologies to evolve crime, thus creating hybrid crime. The emergence of hybrid crime demonstrates how essential it is to identify analytical frameworks that can adapt to evolving environments. In the case of hybrid crime, frameworks must adapt to consider new digital elements, yet must still maintain the capacity to analyze physical actions. This thesis relies on adaptable frameworks to analyze the Silk Road and Silk Road 2.0 investigations by intertwining affordance theory—originally designed to advance ecological psychology—and the concept of stigmergy—originally designed to study ethology. When compared to conventional criminal justice frameworks, affordance theory and stigmergy

have more effectively analyzed dynamic environments relative to changing typologies and disruptive technologies.

3. Not All Technologies Create Criminal Disruption … at Least Not Immediately

New technologies are known to disrupt various markets, but not all Internet technology innovations disrupt crime. For legitimate markets, technology causes disruption when it improves "functionality" and makes something "simpler, cheaper, and more reliable and convenient than mainstream products."[224] Similarly, criminals are always looking for more efficient ways to commit border-related crime. For criminal markets, disruption can happen when Internet technologies significantly change the understood relationship between deviant behavior and criminal justice. As the case studies show, hybrid crime dramatically impacted this causal relationship and made enforcement of border-related crime more difficult. Hybrid crime was possible because of Tor, Bitcoin, and Bitcoin tumbler technologies, but not all of these technologies were disruptive.

The anonymity afforded by Tor has been one of the more difficult challenges for law enforcement to overcome. However, Tor has been available to the public since 2004 and did not become a challenge for law enforcement until 2011, when the Silk Road darknet market was launched.[225] While anonymous communications can help actors conspire, Tor, by itself, could not transition the financial aspects of border-crime from a physical element to a digital one. Tor was not disruptive to crime by itself. The Internet technology that tipped the balance toward the causal relationship was Bitcoin.

Bitcoin was the final technology needed for border crime to evolve. Its technology made anonymous financial transactions possible outside of the normal

---

224 Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Boston, MA: Harvard Business Review Press, 2016), 3581, Kindle.

225 Jeff Stone and Charles Poladian, "Meet the Deep Web: Inside The Hidden Internet That Lies Beyond Google," *International Business Times*, December 31, 2014, Accessed November 18, 2017, http://www.ibtimes.com/meet-deep-web-inside-hidden-Internet-lies-beyond-google-1725784.; Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* (New York, NY: Portfolio/Penguin, 2017), 44.

banking establishment, which in turn allowed illicit money to be hidden in the dark web. Being decentralized, Bitcoin was difficult to track, and illicit monies could flow through the blockchain, transparent to law enforcement, without directly disclosing the buyer or collector's identity. When Ulbricht realized Bitcoin's capabilities, he viewed it in the context of other Internet signifiers to map his darknet market creation to completion. Bitcoin's disruptive power was immediate when it was used as a criminal tool. Although Tor's anonymity affordance has been the most difficult challenge for law enforcement, Bitcoin is what ultimately allowed the creation of darknet marketplaces, which in turn ultimately disrupted border crime and created hybrid crime.

4. Collaboration Helps Overcome Challenges

Investigating hybrid crime requires multiple perspectives and expertise. When investigating the Silk Road and Silk Road 2.0, law enforcement realized that collaboration was essential. No single law enforcement agency had all the expertise to successfully investigate border-related hybrid crime. The HSI and CBP had expertise in identifying, tracking, and seizing packages containing drugs. The IRS could effectively analyze complex evidence. The HSI and DEA knew how to conduct online undercover activity, and the FBI had the most technical expertise in investigating cybercrime. This shared expertise helped law enforcement overcome hybrid crime's arising challenges.

In addition to pooled domestic resources, foreign law enforcement collaboration also proved to be essential. For the Silk Road investigation, the FBI had to rely on foreign counterparts in Iceland to obtain an image of the Silk Road server that ultimately led to Ulbricht's identification. Operation Onymous demonstrated even greater foreign collaboration, and exposed even vaster criminal globalization; at least sixteen foreign countries participated in the darknet marketplace enforcement action. As with the Silk Road investigation, the FBI relied on a foreign counterpart to image a Silk Road 2.0 server that helped identify Benthall. Foreign law enforcement collaboration has proven essential to investigating hybrid crime.

5. "Outsourcing" Hybrid Crime Investigations

Hybrid crime has surpassed enforcement by conventional investigative techniques and has forced law enforcement to seek help from outside technology experts. Despite extensive law enforcement collaboration for both the Silk Road and Silk Road 2.0 investigations, none of the law enforcement agencies had a panacea for countering Tor. The Silk Road 2.0 case study shows that law enforcement recognized it lacked the technological ability to overcome Tor anonymity and sought help from CMU SEI. SEI had the technical capability needed to de-anonymize Tor, which allowed law enforcement to identify Farrell, and likely many other targets of Operation Onymous. A trend has emerged: law enforcement cannot fully investigate hybrid crime without outsourcing investigative elements to those who have unique technical expertise.

SEI is one of forty-three FFRDCs that are actively working on projects deemed important to the government.[226] The projects support both military and civilian government agencies, including the Department of Homeland Security. In addition to academic institutions like CMU, private corporations like RAND and MITRE are also involved in government FFRDC projects.[227] These projects, and especially CMU SEI's research on Tor, demonstrate that Internet technologies have outpaced law enforcement's technical capabilities, and it may be required to outsource investigations to fight hybrid crime. Since Internet technologies are constantly advancing, it is likely that outsourcing will be a continuing trend for law enforcement.

6. Hybrid Crime Creates Unique Challenges but Has Unique Vulnerabilities

Criminal evolution changes the law enforcement–criminal environment by creating new challenges and offering different vulnerabilities. This thesis has already identified challenges that arise when physical criminal elements become digital: how Tor affords anonymity, how Bitcoin makes illicit money difficult to attribute, and how

226 "Master Government List of Federally Funded R&D Centers," National Science Foundation, accessed November 19, 2017, https://www.nsf.gov/statistics/ffrdclist/.

227 Ibid.

tumblers make it even more difficult to trace funds. Despite these pernicious challenges for law enforcement, hybrid crime has also created its own vulnerabilities. The most significant vulnerability surfaces when a physical element becomes digital.

Ulbricht and Benthall implemented Internet technologies handily to create darknet marketplaces, but left digital shadows on the Surface Web that law enforcement used to identify them. Both Ulbricht and Benthall left email address information attached to Internet servers operating marketplaces. Additionally, after Ulbricht integrated Tor, Bitcoin, and Bitcoin tumbler to make the Silk Road, he then had to entice drug vendors and consumers to the darknet marketplace. He did this by posting innocuous but directed messages in online forums on the Surface Web. This public marketing left traces of Ulbricht's identity on the Surface Web that made it possible for law enforcement to link him to the Silk Road.

7. Size Matters

The size and growth of darknet marketplaces impact both criminal levels of risk and law enforcement prioritization. Darknet marketplaces are impacted differently by scalability than legitimate marketplaces. A legitimate marketplace usually requires growth to maintain market share and increase profit. Darknet marketplaces might realize greater profit and illicit market share from growth, but that benefit is counterbalanced by greater risk of arrest. The increased risk comes as a result of more exposure and becoming a more valuable target for law enforcement to pursue.

The Silk Road's growth highlights how risk grew for Ulbricht. When the Silk Road's activity increased, Ulbricht could not fulfill all the operator demands by himself and had to consult and hire additional people to manage basic functions of the website. The growth also resulted in increasing numbers of vendors and buyers who participated in the market, none of whom he knew personally. Ulbricht had no way of knowing whether the people he was dealing with were "friends" of the darknet community, competitors wanting to take over the market, or undercover law enforcement agents. As the case study shows, Ulbricht was unaware some of the people he was dealing with were

undercover agents. It also shows those undercover agents successfully gathered evidence used to convict Ulbricht.

The growth of the Silk Road and Silk Road 2.0 also directly caused law enforcement to pursue the criminal cases. Law enforcement believed that the bigger the marketplace became, the greater the risk it posed to society. Initially, when Ulbricht was facilitating small personal-use quantities of drugs shipped through the U.S. Postal Service, the matter was a low priority for federal law enforcement. Small seizures of personal-use drug quantities are not typically prosecuted federally without extenuating circumstances. When Ulbricht marketed the Silk Road on the Surface Web, he successfully increased his customer base; but in doing so he also attracted the attention of law enforcement and politicians. Benthall sums up the risk he took in scaling-up the Silk Road 2.0 best, stating, "I have no doubt that we have the highest traffic and therefore the highest [law enforcement] crosshairs on our foreheads. … Purchases are going up, vendors are going up—and alongside this, the amount of personal risk staff is taking is exponentially going up. The bigger we become, the more resources agencies are willing to spend on hunting us."[228] Benthall's assessment of the environment was accurate; as the Silk Road 2.0 grew, it became a higher priority for law enforcement.

8. Current Enforcement Efforts Are Not Deterring Darknet Markets

Darknet markets have made it difficult for law enforcement to achieve specific deterrence, and general deterrence has not been achieved. Specific deterrence involves changing an individual's behavior so he or she does not want to, or cannot, commit future crimes due to incarceration or other punishment. General deterrence, however, means changing group behaviors, causing larger criminal groups to realize the risks of crime are greater than the rewards. General deterrence can be the result of aggressive enforcement or a single case of specific deterrence (such as an individual criminal's severe sentence) that dissuades others from wanting to commit the same criminal act. General deterrence is the ultimate goal for law enforcement because the overall benefit to society is less crime. Although law enforcement aims to achieve general deterrence for all types of

[228] United States v. Blake Benthall, Sealed Complaint, 16.

crimes, including border-related crimes, it does not always effectively do so. It has been especially challenging to foster general deterrence for border-related crimes facilitated by the Internet.

There have been various studies on law enforcement's efforts to stop darknet marketplaces. These studies have consistently shown that after a large darknet marketplace is seized, use of darknet marketplaces immediately decreases. However, the decrease is only temporary; eventually, the users are displaced to other marketplaces. One study published in the *International Journal of Cyber Criminology* looked at the behavior of darknet market users and concluded enforcement displaced criminal activity, but did not significantly deter it.[229] The authors of the study gathered data from content analysis of an online forum established immediately after the Silk Road marketplace was seized.[230] Figure 5 shows conclusions drawn from the question: "Did the users still believe in the viability of Dark Net markets, after Silk Road closure?"[231] The results show that relatively few users were dissuaded altogether from using darknet marketplaces.

[229] Wesley Lacson and Beata Jones, "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road," *International Journal of Cyber Criminology* 10, no. 1 (January–June 2016): 52.

[230] Ibid.

[231] Ibid.

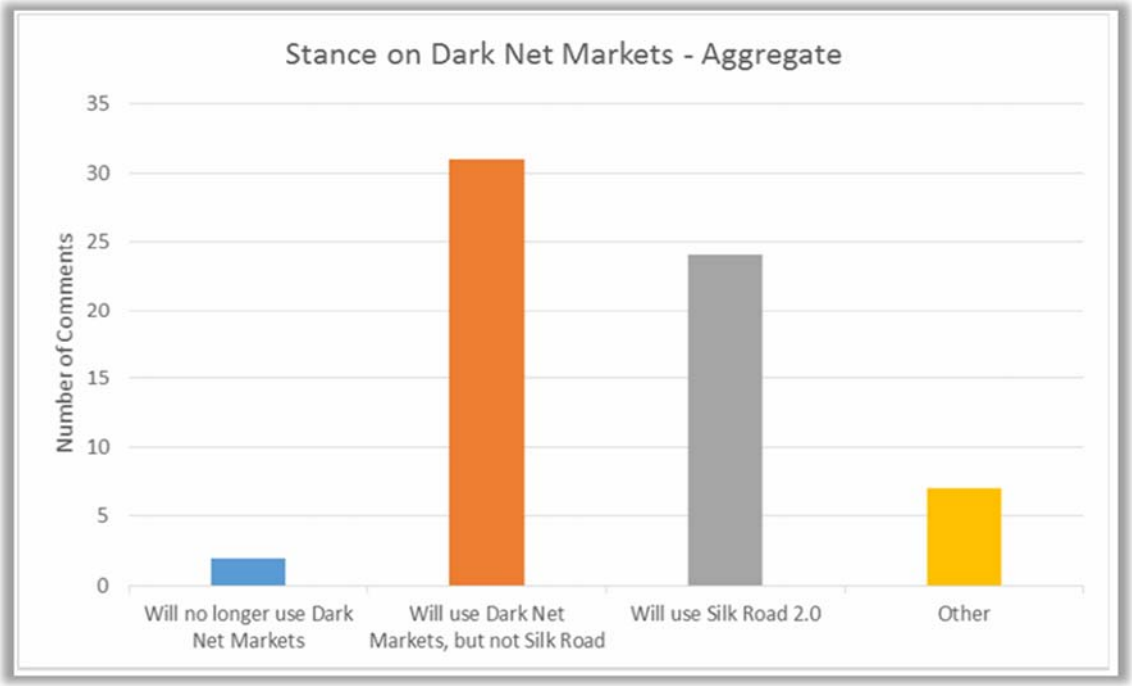

Figure 5. Darknet Market Displacement after Enforcement[232]

A second study, published in the *Crime Law and Social Change Journal*, looks at the Agora, Cloud 9, Evolution, Hydra, and Silk Road 2.0 darknet marketplaces before and after three of the sites were seized during Operation Onymous.[233] This study demonstrates the effect of darknet marketplace enforcement efforts by analyzing the supply and demand of drugs bought and sold in the dark web around the time period of Operation Onymous. The study concluded that the activity of buying and selling drugs was impacted by marketplace seizures, but drug prices were left unchanged. Additionally, even when activity was impacted by seizures, the effect was only temporary. Figure 6 shows the number of active dealers on the five marketplaces before and after Operation Onymous as a way of demonstrating how the supply side was impacted by enforcement. This chart shows a drastic reduction in the number of dealers immediately after Hydra, Cloud 9, and Silk Road 2.0 sites were seized, but it also shows an eventual spike in dealer activity at Evolution.

232 Source: Lacson and Jones, "The 21st Century DarkNet Market," 52.

233 Décary-Hétu and Giommoni, "Police Crackdowns," 66.

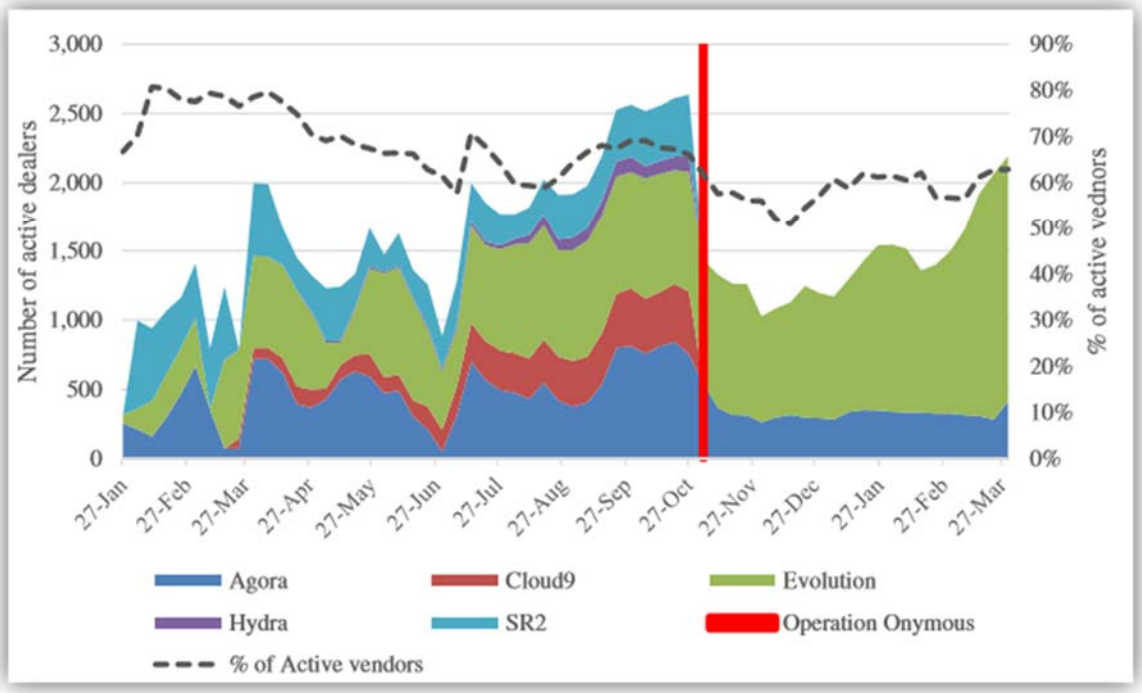

Figure 6. Supply-Side Impact of Darknet Market Enforcement[234]

The same study viewed feedback loops as a way to determine how the demand side was impacted by Operation Onymous. Figure 7 shows how feedback loops were impacted after law enforcement seized the Cloud 9, Hydra, and Silk Road 2.0 sites. The study presumes the changes in feedback loops translate to the amount of illegal drugs being sold. Using this presumption, overall drug sales decreased for a short time after the seizures and then rebounded significantly when displaced to the Evolution marketplace.

234 Source: Décary-Hétu and Giommoni, "Police Crackdowns," 66.

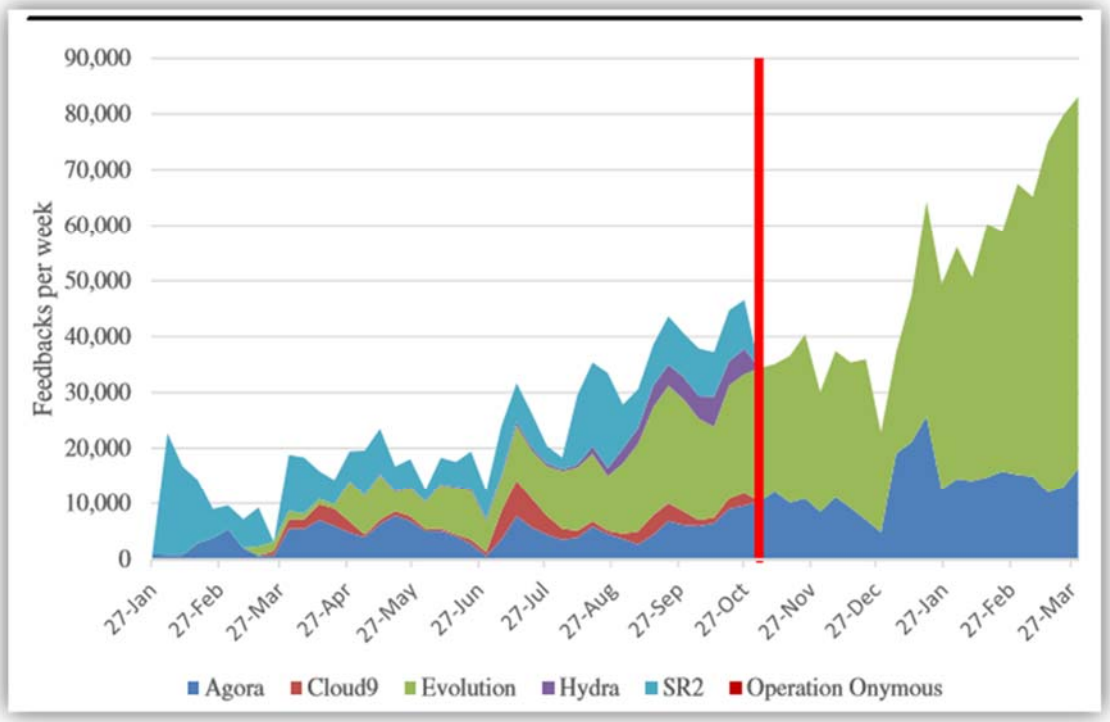

Figure 7. Demand-Side Impact of Darknet Market Enforcement[235]

A third study, conducted at the National Drug and Alcohol Research Centre in New South Wales, Australia, shows darknet markets were impacted only temporarily by enforcement efforts.[236] From October 2013 to November 2015, researchers gathered data from thirty-nine darknet markets that showed significant decreases in vendor activity after Operation Onymous, and then again after the Evolution site was closed from an exit scam. Figure 8 demonstrates vendor activity during three distinct periods. Period 1 starts when the Silk Road was seized and ends shortly after Operation Onymous. The second period begins shortly after Operation Onymous until the Evolution exit scam. The final period shows vendor activity after the Evolution marketplace closure.

[235] Décary-Hétu and Giommoni, "Police Crackdowns," 69.

[236] Joe Van Buskirk et al., "The Recovery of Online Drug Markets Following Law Enforcement and other Disruptions," *Drug and Alcohol Dependence* 173 (2017): 160, doi:10.1016/j.drugalcdep.2017.01.004.

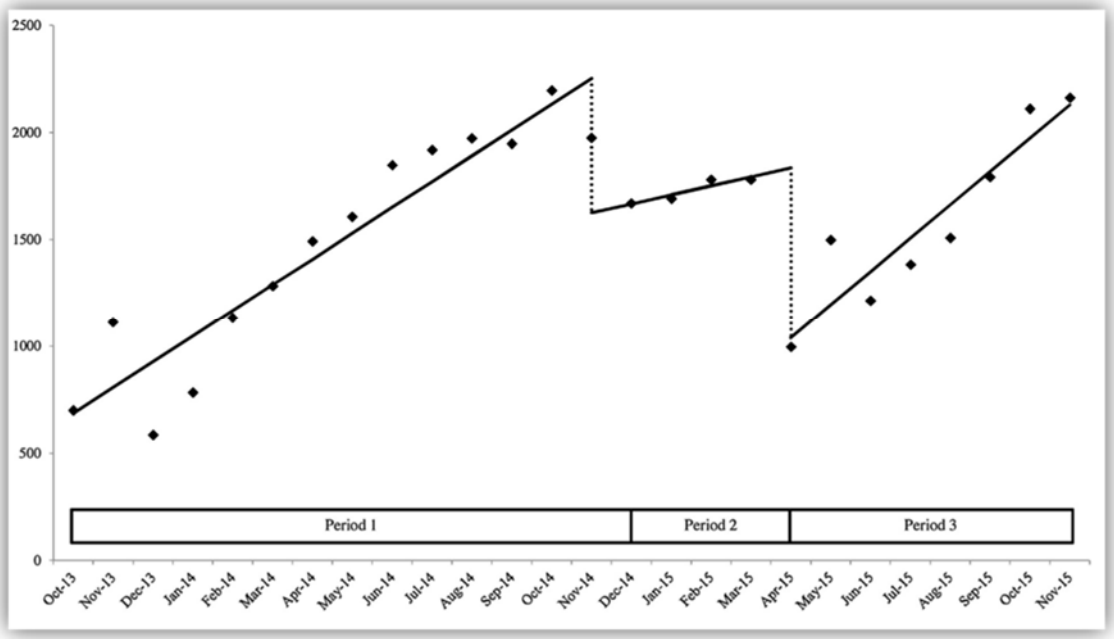

Figure 8. Darknet Market Vendor Activity after Enforcement and Exit Scam[237]

This chart shows drops in vendor activity after the Silk Road seizure, Operation Onymous, and Evolution closure. While these drops are dramatic, vendor activity continued to climb and, by the time the study concluded, was at near all–time activity highs. One point of interest is that the largest decrease of activity did not stem from enforcement efforts, but from a loss of trust when Evolution's exit scam occurred. Displacement from other darknet marketplaces to Evolution may have contributed to this large decrease in activity.[238]

These three studies demonstrate how difficult it is to deter criminal activity from darknet marketplaces. While specific deterrence has been shown against individual criminal actors and marketplaces, general deterrence has not been acheived. Enforcement efforts have been effective at temporarily decreasing and displacing criminal activity, but have not resulted in less criminal activity overall. Additionally, there is no indication that enforcement activity aimed at darknet marketplaces has displaced criminal activity from

[237] Source: Van Buskirk et al., "Recovery of Online Drug Markets," 160.

[238] Van Buskirk et al., "Recovery of Online Drug Markets," 160.

the digital realm back to the physical. This chapter's three studies review darknet marketplace activity from the Silk Road through the time period immediately following the Evolution exit scam, which ended in November 2015. The next chapter concludes the discussion by showing the present state of hybrid crime and by providing recommendations for law enforcement based on the research findings. Recent cases show that the category of hybrid crime has become the staple of drug smuggling and that the intermixing of digital and physical elements is impacting other border-related crimes as well.

VII. PRESENT ENVIRONMENT, RECOMMENDATIONS, AND CONCLUSIONS FOR FUTURE RESEARCH

> Make no mistake, the forces of law and justice face a new challenge from the criminals and transnational criminal organizations who think they can commit their crimes with impunity using the dark net. The dark net is not a place to hide...I believe that because of this operation, the American people are safer-safer from the threat of identity fraud and malware, and safer from deadly drugs.
>
> —Attorney General Jeff Sessions[239]
> Regarding the arrest of Alexandre Cazes and seizure of AlphaBay

Although law enforcement has been continuously investigating hybrid crimes and darknet markets since the Silk Road first emerged, the challenges from Internet technologies used to facilitate cross-border crime have not been curtailed. Recent arrests show that hybrid crime has become the new standard for drug trafficking, and darknet markets have become an international dilemma. Cross-border crimes like child sexual exploitation and money laundering are also directly impacted by the shifting balance between physical and digital crime elements. This chapter explains the present status of hybrid crime and recommends law enforcement tactics that can counter present and future challenges. The first section of this chapter identifies and briefly describes some of the most recent cases involving hybrid crime, contextualizing why those cases are of interest to this study. The second section provides law enforcement and criminal justice professionals with short-, medium-, and long-term recommendations for managing the challenges of hybrid crime. The final section introduces avenues for future research that may advance the study of upcoming challenges.

A. PRESENT STATUS OF HYBRID CRIME

As crimes continue to evolve and include more digital elements, law enforcement has also been adapting its strategies. This evolution–adaptation response is a perfect

239 "AlphaBay, the Largest Online 'Dark Market' Shut Down," Department of Justice, July 20, 2017, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

example of the stigmergic cycle in action, and shows the continuing dynamic relationship between law enforcement and criminals. The following case examples not only show this evolution and adaptation, but also illustrate several of the findings noted in Chapter VI. The examples highlight collaboration, enforcement efforts aimed at hybrid crime vulnerabilities, cryptocurrencies as disruptive technology, and the necessity to incorporate non–law enforcement technology expertise into hybrid crime investigations.

1. Operation Hyperion

Operation Hyperion was a global law enforcement effort involving HSI, CBP, FBI, DEA, and more than nine foreign counterparts, including law enforcement from Australia, New Zealand, Canada, and the United Kingdom.[240] Law enforcement went on the offensive from October 22, 2016 to October 28, 2016, by identifying vendors and buyers of drugs hidden in the dark web.[241] CBP and HSI focused efforts on interdicting mail shipments containing illegal goods.[242] The FBI interviewed over 150 individuals suspected of receiving mail shipments of illegal goods.[243] Because the operation focused on warning people about the dangers of darknet markets for illegal activity, rather than on enforcement, there were no reports of domestic arrests or seizures.[244] Although U.S. law enforcement did not report substantial results, foreign governments substantiated that the goal of the operation was to provide a warning about darknet marketplaces.

During the operation, law enforcement tried to dissuade the public from using darknet markets by proving they could not be trusted. Law enforcement demonstrated—and publicized—that enforcement agencies could identify presumably "anonymous" individuals operating on the dark web. The Dutch National Prosecution Service and

240 "Law Enforcement Agencies around the World Collaborate on International Darknet Marketplace Enforcement Operation," ICE, accessed October 29, 2017, https://www.ice.gov/news/releases/law-enforcement-agencies-around-world-collaborate-international-darknet-marketplace.

241 Ibid.

242 Joseph Cox, "'Operation Hyperion' Targets Suspected Dark Web Users around the World," *Motherboard*, November 03, 2016, https://motherboard.vice.com/en_us/article/z438d8/operation-hyperion-targets-suspected-dark-web-users-around-the-world.

243 Ibid.

244 Ibid.

Dutch police posted the online identities of a large number of vendors selling illegal drugs, as well as buyers who had already been arrested on a dark website created by the government.[245] Swedish police "claimed to have identified some 3,000 suspected buyers," initiated 176 investigations, and detained several people in connection with darknet market drug smuggling.[246] New Zealand police interviewed 160 people and the Royal Canadian Mounted Police arrested a person suspected of narcotics trafficking.[247] While none of these results demonstrate significant enforcement actions, they show international law enforcement collaboration undermining the trust of darknet marketplaces. While Operation Hyperion can be viewed as a law enforcement strategy to deter hybrid crime, it may also be seen as a prelude to the take-downs of AlphaBay and Hansa.

Operation Hyperion is important because it demonstrates law enforcement efforts aimed at influencing media dependency, as explained by media dependency theory, and shows a recognition that domestic and worldwide law enforcement collaboration is required to counter hybrid crime.

2. AlphaBay

AlphaBay was the largest darknet marketplace in history; its operators and users demonstrated continued use of Internet technologies to facilitate border-related crime. AlphaBay was a law enforcement priority because of its scale, but also because it was facilitating the sale of fentanyl, which was causing overdose deaths.[248] The investigation

---

[245] Sarah Jamie Lewis, "Operation Hyperion: Netherlands Law Enforcement Troll Dark Market Vendors," *Mascherari Press*, March 27, 2017, https://mascherari.press/operation-hyperion-netherlands-law-enforcement-troll-dark-market-buyers/.

[246] Cox, "Operation Hyperion"; Benjamin Vitáris, "176 Investigations Started in Sweden, Operation Hyperion," *Deep Dot Web*, January 9, 2017, https://www.deepdotweb.com/2017/01/06/176-investigations-started-norway-operation-hyperion/.

[247] Cox, "Operation Hyperion."

[248] Nathaniel Popper, "Opioid Dealers Embrace the Dark Web to Send Deadly Drugs by Mail," *New York Times*, June 10, 2017, https://www.nytimes.com/2017/06/10/business/dealbook/opioid-dark-web-drug-overdose.html.

was primarily conducted by the FBI and DEA under an operation named Bayonet.[249] The IRS, HSI, and multiple international partners assisted with the investigation.[250] The investigation revealed the marketplace was operated by a Canadian citizen named Alexandre Cazes, also known by the online pseudonym ALPHA02.[251] AlphaBay linked 40,000 vendors to over 200,000 users and had over 250,000 listings for illegal drugs.[252] Even though AlphaBay was vastly larger than the Silk Road and Silk Road 2.0, Cazes relied on the same Internet technologies, Tor and Bitcoin, to maintain anonymity.[253] Unlike the Silk Road, AlphaBay also accepted the newer cryptocurrencies of Monero and Ethereum for illicit transactions.[254]

AlphaBay operated from December 2014 until July 2017, when the marketplace was seized and Cazes arrested in Thailand.[255] Like Ulbricht, Cazes was identified due to difficulties he encountered when transitioning a physical crime into a hybrid crime. While the technologies maintained anonymity, Cazes was reportedly identified from digital shadows; his personal Hotmail email address was discovered in the header of AlphaBay welcome and password recovery emails.[256] Cazes was not ultimately prosecuted; shortly after arrest he committed suicide in a Bangkok, Thailand, jail.[257] In addition to Cazes' arrest, law enforcement seized millions of dollars of cyptocurrency

---

249 "Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation," Europol, July 20, 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

250 "AlphaBay, the Largest Online 'Dark Market,' Shut Down," U.S. Department of Justice, July 20, 2017, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

251 Ibid.

252 Ibid.

253 Ibid.

254 Ibid.

255 Andrea Bellemare, "The Secret Life of Alexandre Cazes, Alleged Dark Web Mastermind," CBC News, August 16, 2017, http://www.cbc.ca/news/canada/montreal/alexandre-cazes-millionaire-cars-property-alphabay-1.4215894.

256 Ibid.

257 Andrew Blake, "Suspected AlphaBay Operator Found Dead in Thai Jail Cell Awaiting Extradition," *Washington Times*, July 14, 2017, https://www.washingtontimes.com/news/2017/jul/14/alexandre-cazes-suspected-alphabay-operator-found-/.

and servers in Canada and the Netherlands.[258] The seizure of the website immediately caused criminal displacement from AlphaBay to Hansa.[259]

The recent takedown of AlphaBay is of interest to this study for three reasons. First, this case demonstrates how increased scalability made AlphaBay a prioritized target for law enforcement efforts. Second, because law enforcement identified the operator of AlphaBay by tracking his digital shadow, this case highlights the pervasiveness of the vulnerability posed to hybrid crimes when physical criminal elements are transitioned to digital counterparts. Third, the closure of AlphaBay was not met with general deterrence, but instead resulted in displacement to the Hansa darknet market. While this reaction supports the finding that general deterrence is not being achieved, displacement in this case is even more important because it was used as part of a law enforcement strategy, as explained in the following section.

3. Hansa

The Hansa investigation was led by the Dutch police, with support from Europol.[260] Hansa was found to be operated by two German nationals using servers in the Netherlands, Germany, and Lithuania.[261] Unlike AlphaBay, the Hansa operators tried to make their darknet marketplace less of a priority for law enforcement by forbidding the sale of fentanyl, but its large scale still attracted law enforcement's attention. The most compelling aspect of the Hansa investigation was how the Dutch police turned the marketplace into a honeypot to track and identify users being displaced from the seizure of AlphaBay.[262]

The Dutch police covertly operated Hansa for one month, including two weeks immediately following the seizure of AlphaBay, to monitor and record user movements

---

[258] Europol, "Massive Blow to Criminal Dark Web Activities."

[259] Blake, "Suspected AlphaBay Operator Found Dead."

[260] Europol, "Massive Blow to Criminal Dark Web Activities."

[261] Ibid.

[262] Ibid.

from one marketplace to the other.[263] Hansa saw "an eight-fold increase ... recorded immediately following the shutdown of AlphaBay."[264] The honeypot strategy generated approximately 10,000 leads against drug buyers, which were provided to Europol.[265] The Dutch police officially closed the Hansa marketplace on July 20, 2017.[266]

As with the Silk Road 2.0 investigation, law enforcement investigating Hansa obtained technological expertise from non–law enforcement sources; the Dutch police and Europol relied on a company named Bitdefender.[267] Bitdefender is a private Internet security company headquartered in Romania that provides cybersecurity protections to over 500 million users around the world.[268] European authorities relied on Bitdefender to "compile the technical evidence that led to the shutdown of Hansa."[269] This is another example of how technological complexities used to facilitate hybrid crime require outsourced law enforcement response.

In addition to showing global collaboration, the Hansa investigation exemplifies how law enforcement can adapts its investigative techniques—investigators successfully turned the darknet marketplace into a honeypot and outsourced technical investigative components to overcome the challenges presented by hybrid crime.

4. BTC-e Money Laundering

Alexander Vinnik, a thirty-seven-year-old Russian national, was arrested in Greece on July 25, 2017, on a twenty-one-count indictment issued from the Northern

263 Ibid.

264 Ibid.

265 Europol, "Massive Blow to Criminal Dark Web Activities."

266 Ibid.

267 Ibid.

268 "Latest News: Bitdefender Founder Florin Talpeș: 2017's Most Admired CEO in Romania," Bitdefender, accessed November 19, 2017, https://www.bitdefender.com/news/bitdefender-founder-florin-talpe%C8%99:-2017%E2%80%99s-most-admired-ceo-in-romania-3378.html.

269 Ibid.

District of California.[270] Vinnik was charged with multiple crimes, including international money laundering and operating an unlicensed money service business.[271] Vinnik's arrest was the culmination of investigative efforts by the IRS, HSI, FBI, Secret Service, Federal Deposit Insurance Corporation, and Financial Crimes Enforcement Network (FinCEN).[272] Starting in 2011, Vinnik allegedly laundered over $4 billion in Bitcoins through a digital currency exchange company he operated called BTC-e.[273] In addition to Bitcoin, BTC-e exchanged litecoin, ethers, worldcoin, dogecoin, and fiat currencies.[274] Vinnik's money laundering service made it possible for criminals to make cybercrime lucrative; available services ranged from "computer hacking, to fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking."[275] The BTC-e exchange service was designed to allow physical and digital elements to be segmented and kept anonymous. A BTC-e user would not have to provide any personal information to open an account, but also could not wire money directly into BTC-e.[276] Money had to first be wired to a shell company and then converted into cryptocurrency before it was transferred into BTC-e, forming a separation between an individual's identity and BTC-e's anonymity.[277]

Vinnik maintained shell companies in Singapore, the British Virgin Islands, France, and New Zealand.[278] He had customers worldwide, including in the United States. Two U.S. customers were directly linked to the original Silk Road investigation: DEA Agent Carl Mark Force and Secret Service Agent Shaun Bridges laundered

270 "Russian National and Bitcoin Exchange Charged In 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox," U.S. Department of Justice, July 26, 2017, https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

271 Ibid.

272 Department of Justice, "Russian National and Bitcoin Exchange."

273 Ibid.

274 United States v BTC-E, A/K/A Canton Business Corporation and Alexander Vinnik, Superseding Indictment, Case #CR16-00227 SI (ND CA, January 17, 2017), 3.

275 Department of Justice, "Russian National and Bitcoin Exchange Charged."

276 United States v BTC-E and Alexander Vinnik, 9–10.

277 Ibid., 10.

278 Ibid., 3.

hundreds of thousands of dollars in stolen Bitcoin through BTC-e.[279] Both agents worked on the Baltimore Silk Road Task Force and stole large amounts of Bitcoin from the Silk Road through corrupt acts.[280] For their illegal acts, Force and Bridges were convicted of various financial-related charges and will remain incarcerated until 2022.[281] Vinnik, unlike Force and Bridges, has not yet been prosecuted and is contesting extradition to the United States.[282] The case against Vinnik is the largest money laundering investigation of its kind and exemplifies the continuing disruptive power that cryptocurrency technology has on border-related crime.

The BTC-e case shows that money laundering is no longer a physical crime based on bulk cash smuggling or wire transfers. Cryptocurrencies are disrupting the criminal environment and previously understood notions of money laundering. As a result, hybrid crime is beginning to evolve the border crime of international money laundering just as it evolved drug trafficking.

5. Human Trafficking and Sexual Exploitation

In addition to analyzing the Internet-related evolution of drug trafficking and money laundering, this thesis also reviewed how human trafficking and sexual exploitation are facilitated by Internet technologies. Research indicates that criminals have used Tor and Bitcoin to anonymize transfers of sexually explicit videos, photographs, and live streams, but not to facilitate border-related human trafficking.[283] It appears to be a more common trend for facilitators of domestic prostitution—but not

279 Ibid, 12.

280 Ibid., 12–13.

281 Bilton, *American Kingpin*, 319.

282 Ibid., 317–319; Dan Boylan, "U.S., Russia Fight over 'Brain' of Bitcoin Crime Suspect Alexander Vinnik," *Washington Times,* October 8, 2017, www.washingtontimes.com/news/2017/oct/8/alexander-vinnik-bitcoin-crime-suspect-at-center-o/.

283 Human trafficking has different definitions for different jurisdictions and levels of government. It involves the movement of people by force, fraud, or coercion to obtain some type of labor or commercial sex act. For this thesis, only crimes having a transnational nexus and use of Internet technologies were considered for inclusion. "What Is Human Trafficking?" Department of Homeland Security, November 21, 2016, https://www.dhs.gov/blue-campaign/what-human-trafficking.

those of transnational human trafficking—to rely on Internet technologies like Tor.[284] Since human trafficking was not found to be significantly facilitated by Internet technologies, it appears to remain more a physical than hybrid crime.

Even though the various elements of transferring sexually explicit videos, photographs, and live streaming may include digital and physical elements, and have a border nexus, these types of crimes are traditionally classified as cybercrimes. As mentioned previously, classifying crime is not easy and there are many variables. Whether a crime is categorized as hybrid instead of cyber would depend on the level of physical movement of people or goods. Despite sexual exploitation cases not neatly fitting into the label of hybrid crime, some were found to rely on affordances from Tor and BitTorrent. Others are not as sophisticated and rely on simple Internet access. In impoverished countries like the Philippines, expanded access to the Internet has sparked an explosion of cybersex dens as a way to generate income.[285] These cybersex dens are producing live streams of young children being sexually abused for paying pedophiles in places like the United States, Australia, and Europe.[286]

The HSI and FBI have assisted law enforcement in the Philippines with investigations of numerous child sexual abuse cases conducted at the hands of family members, other Philippine nationals, and foreign nationals. The abuse is recorded and streamed online in videos to paying pedophiles. Some instances include:

- In July 2013, HSI assisted Philippine authorities with investigating, locating, and arresting Maybel Oranga, Bryan Sagmit, and Christian Chameco for running a cybersex den in Malabania, Angeles City,

[284] DARPA's MEMEX program has been used to help gather evidence from the dark web for state prosecutions of sex trafficking for the New York District Attorney's office; Larry Greenemeier, "Human Traffickers Caught on Hidden Internet," *Scientific American*, February 8, 2015, 5, http://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-Internet/.

[285] Martha Mendoza and Jim Gomez, "Philippine Police Make More Arrests, Rescues in Live-Streaming of Child Porn to U.S.," *Chicago Tribune*, May 12, 2017, http://www.chicagotribune.com/news/nationworld/ct-philippines-cybersex-arrests-rescues-20170512-story.html.

[286] Ibid.

Pampanga.[287] Three female victims, ages fifteen, sixteen, and seventeen were rescued.[288]

- In September 2013, HSI assisted Philippine authorities with investigating, locating, and arresting Maricel Ayad and Dinesio Encallado Inoc for operating a webcam sex tourism operation in Cordova, Cebu.[289] Three female victims, ages two, nine, and eleven, were rescued.[290]

- In April 2017, the FBI assisted Philippines authorities in the city of Mabalacat with arresting U.S. citizen David Timothy Deakin for abusing children and operating a cybersex den.[291] He relied on Tor, BitTorrent, and live streaming to operate webcam sex tourism.[292] Deakin has been charged with cybercrime, child pornography, child abuse, and child trafficking.[293]

These cases show the present status of border-related sexual exploitation crimes facilitated by the Internet. Although the crime is appropriately categorized as a cybercrime, the crimes could be adapted to fit the hybrid mold. For instance, a pedophile may use Internet technologies to locate images of sexual exploitation, and then *follow* those images by physically traveling to a foreign country to engage in illicit sexual conduct. The act of physically traveling to facilitate the crime would change the balance

287 "ICE Works with Philippine Law Enforcement to Capture Cybersex Operators and Rescue Child Victims," ICE, accessed November 8, 2017, https://www.ice.gov/news/releases/ice-works-philippine-law-enforcement-capture-cybersex-operators-and-rescue-child.

288 Ibid.

289 ICE, "ICE Works with Philippine Law Enforcement."

290 Ibid.

291 "Inside the Raid on a Suspected Pedophile's Cybersex Den," CBS News, May 12, 2017, https://www.cbsnews.com/news/child-cybersex-abuse-webcam-philippines-pedophile-suspect-david-timothy-deakin/.

292 Ibid.

293 "American Expat Nabbed in Child Porn Bust in Philippines," *NY Daily News*, May 9, 2017, http://www.nydailynews.com/news/world/american-expat-nabbed-child-porn-bust-philippines-article-1.3149392.

of physical and digital elements; the crime would then more appropriately be classified in the hybrid category.

B. RECOMMENDATIONS

This study set out to answer a descriptive question, yet the overall goal was to explore unique ways of viewing, understanding, and fighting crime. To that end, this section provides prescriptive recommendations meant to improve investigative strategies for law enforcement and to advance the study of criminal justice. For ease of implementation and adaptability, the recommendations are divided into short-, medium-, and long-term strategic goals. While portions of the strategies are based in theory, they are not meant to be lost in theoretical discussions; they should be used for practical applications to fight crime. The following strategies are derived from and focus on hybrid crime, but can be applied to other types and categories of crime.

1. Short-Term Strategy Recommendations

Short-term strategy recommendations are aimed at overcoming the immediate challenges presented by border-related crimes facilitated by Internet technologies. The recommendations are designed specifically to help law enforcement practitioners understand and manage the current dynamic environment. This strategy could be considered reactive because it is aimed at maintaining law enforcement's current position within the stigmergic cycle rather than trying to change the law enforcement–criminal balance. The four recommendations in the short-term strategy build upon one another: technology training, emphasis on properly classifying crime, smart enforcement, and government collaboration.

a. Technology Training

To understand the hybrid criminal environment, investigators must first learn about related technologies that may facilitate crime. As crime evolves and more elements become digital, mindsets must change; training previously reserved for investigators of cybercrimes must be provided to all investigators. Tor, Bitcoin, Bitcoin tumblers, peer-to-peer networks, encryption systems, and BitTorrent are just some of the technologies

investigators must understand if they are to simply recognize when crimes are being facilitated by technology. Once a baseline understanding of technology is achieved, law enforcement can then focus on effective responses. One of the most significant results of understanding technology and recognizing crime facilitated by that technology is being able to properly classify crime.

b. Classifying Crime

Properly classifying crime is the second recommendation for the short-term strategy and extremely important for determining responses, strategy, techniques, and analysis processes. While classifying a crime is not always an easy undertaking, it is essential that law enforcement considers labeling a part of the investigative process. The purpose of classifying is not to "pigeon-hole" a crime into a category for bureaucratic documentation and simplification; it is actually the reverse. The purpose of thinking about criminal categories is to open investigators' minds about evolving crime, new possible categories, and overall criminal typology. Whether a crime is labeled physical, cyber, or hybrid will help determine the type of investigative strategy used to respond or the type of expertise needed for support. Similarly, determining whether a deviant act is labeled drug smuggling, human trafficking/sexual exploitation, or money laundering will help determine the type of investigative techniques employed. While all investigations and crimes may have similarities or overlap, subtle differences are important. If a crime is properly labeled, law enforcement can focus on the established strategies and techniques that most effectively and efficiently counter that particular crime. As a secondary but equally important matter, proper labeling will also enable holistic analysis performed through sociological or technological frameworks.

c. Smart Enforcement

The third recommendation, after properly labeling crime, is to develop and employ smart enforcement techniques. Smart enforcement techniques involve a combination of traditional and unconventional techniques to overcoming many of the hybrid crime challenges. As an example, traditional techniques do not effectively uncover a suspect's identity when it is anonymized by Internet technologies, but are still effective

when employed against the vulnerability that occurs when physical crime elements become digital. When the elements are transitioning, investigators can search for digital shadows on the Surface Web to help identify an anonymized suspect in the dark web. In addition to using traditional techniques, law enforcement should always seek unconventional methods to de-anonymize Tor and capitalize on the legal precedent that anonymizing software is not afforded privacy protections.

d. Government Collaboration

The fourth short-term recommendation is to advance law enforcement collaboration. Globalization of crime has made it essential to work investigations across multiple jurisdictions and borders. Collaboration is no longer an option, but an investigative necessity. Additionally, as law enforcement agencies learn to adapt techniques to counter hybrid crime, cooperative efforts are one of the best ways to immediately overcome hybrid crime challenges. No one agency has all the tools for success, but cumulative expertise between local, state, federal, and international agencies leverages investigative strengths.

2. Medium-Term Strategy Recommendations

The medium-term strategy should begin after law enforcement has made successful progress toward implementing the short-term strategy items. Recommendations for medium-term strategy are intended to complement and advance the short-term strategy by transitioning law enforcement from a reactive to proactive posture. In terms of the stigmergic cycle, this strategy would make it so law enforcement is pushing the cycle instead of being pushed by it. In other words, by maintaining a proactive posture, law enforcement might have more influence over self-organization of the decentralized law enforcement–criminal environment. The medium-term strategy recommendations include building on law enforcement collaboration by engaging public–private partnerships and refining the smart enforcement strategy to focus more efforts on general deterrence. This medium-term strategy is primarily implemented by law enforcement practitioners, agency heads, and other government decision makers.

a. Public–Private Partnerships

The first middle-term recommendation is to expand collaboration beyond the law enforcement community by creating public–private partnerships. This type of collaboration is essential to managing the technological advancements used to commit crime. Similar to the DOD's partnership with CMU SEI, Europol's partnership with Bitdefender, and DARPA's use of various academic institutions to advance the MEMEX program, the Department of Justice and Department of Homeland Security should establish their own FFRDC designed to research the future technological evolution of crime.[294] This type of collaboration would provide the needed support to advance law enforcement's understanding of technology faster than criminal adaptations. Without such a public–private partnership, future Internet technology adaptations will likely afford new criminal methods and diminish law enforcement's capacity to investigate crime. If this were to occur, law enforcement would regress in the stigmergic cycle and no longer maintain a proactive enforcement posture.

b. Smart Enforcement (Phase 2)

The second recommendation is to advance the smart enforcement technique beyond the short-term recommendations and modify it to achieve general deterrence. General deterrence against darknet marketplaces has not been achieved in the past by arrests and seizures alone, but is possible through an aggressive strategy aimed at diminishing the public's trust in these marketplaces. As noted in Chapter III, media dependency theory explains how social network acceptance has created a level of social trust for darknet markets. If law enforcement can diminish trust in the markets, the public may be deterred from using them. The tactical elements to diminish trust include: seizing cryptocurrencies from marketplaces in a way that makes it appear the money was stolen, using website attacks to cause site failures, and initiating publicity campaigns appearing to come from within forum communities that generate concerns over site security, operator trustworthiness, and anonymity protections.

---

294 United States v Brian Farrell, Order on Defendant's Motion to Compel, 1–2; Europol, "Massive Blow to Criminal Dark Web Activities"; TedxTalks, "Christopher White," YouTube video, 14:16.

The collapse of the darknet marketplace Evolution exemplifies how this strategy will work. Evolution facilitated an estimated 475,000 transactions a year worth over $52 million.[295] It also had over 28,000 users connected to its social forum.[296] In March 2014, Evolution's unidentified operators initiated an exit-scam by shutting down the website and stealing approximately $12 million in customer funds.[297] The exit-scam resulted in a larger decrease of illicit vendor activity than all the law enforcement actions of Operation Onymous.[298] In essence, this law enforcement strategy is an attempt to achieve general deterrence by implementing law enforcement–sponsored exit scams.

3. Long-Term Strategy Recommendation

Long-term recommendations complement both the short- and medium-term strategies by building sustainability. These recommendations could be implemented at any stage of progress within the other two strategies, but should be viewed as long-term processes from the beginning. This level of strategy is important for law enforcement practitioners, agency heads, oversight committees, academia, think tanks, and anyone else studying criminal justice to consider. The long-term strategy recommendations include building a law enforcement mindset that technology is "one with crime" and incorporating unconventional frameworks to analyze crime.

a. Technology Mindset

Building a mindset that technology is "one with crime" is essential to investigating both present and future crimes. Providing training to agents, officers, and investigators is only the first step toward building the mindset. Training needs to be followed by access to technological tools. Computer forensic analysis is no longer a specialty; a certain level of forensic knowledge is required for all investigations. Specialty software designed to gather and analyze evidence should be prevalent.

295 Thomas Fox-Brewster, "A $50m Drug and Gun Dark Web Market Just Disappeared and Millions in Bitcoin with It," *Forbes*, March 23, 2015, https://www.forbes.com/sites/thomasbrewster/2015/03/18/evolution-market-a-scam-says-site-pr/#5f23f90d780f.

296 Ibid.

297 Joe Van Buskirk et al., "Online Drug Markets," 160.

298 Ibid.

Platforms for conducting online undercover activity should be established and ready to use. Policies and procedures for using cryptocurrencies as an investigative tool should be simple and supported. Tor should not be a mystery or something to fear accessing. While training is extremely beneficial, a technology mindset cannot be built if tools are not provided

The next step toward building a one-with-crime technology mindset is for agencies to implement future studies into present and future strategies. Agents, officers, and investigators should be taught the basic approaches of future studies; though they do not all need to become futurists, they should advance the mindset. The reactive practice of identifying new technologies only *after* those technologies stymie investigative progress should end. Agency heads should start hiring trained futurists, specifically to research technology and crime. Their job would be to perceive new affordances ahead of criminals. A futurist would also be able to assess which technologies could potentially be disruptive to the law enforcement–criminal environment, distinguishing them from technologies that are new, but manageable. The goal would be to identify potential technological challenges early in the cycle so research taskings can be referred to FFRDCs to develop tools before they are needed.

b. Frameworks

The final recommendation for the long-term strategy is to use unconventional frameworks to analyze crime. New frameworks, outside the traditional sociological sphere, must be included into the study of criminal justice to analyze technology's ever-changing role in crime. The frameworks need to be adaptable for the dynamic environment and directly applicable to law enforcement. Affordance theory and the concept of stigmergy are recommended for this strategy because, rather than simply predicting deviant behavior, they can help law enforcement understand the tools that may be used for deviant behavior. Gaining an understanding of objects (technologies) and what those objects can do for crime (affordances) is immediately important for the fight against crime.

These short-, medium-, and long-term strategy recommendations are a starting point; they can begin to help law enforcement better manage the dynamic environment of technology and crime. While these strategies are intended for border-related crime they may serve as a roadmap for many other criminal focuses. Despite touching on theory and sociological concepts, this strategy is not intended to advance the study of criminology by determining causes of deviant behavior. Instead, it is intended to support the study of criminal justice by providing immediate practical benefits for law enforcement.

C. CONCLUSION AND FUTURE RESEARCH

The Internet is going to grow in size, capability, and use. The Internet of things is expected to raise the number of devices connected to the Internet to 25 billion by 2020.[299] Currently, 3.8 billion people across the globe have Internet access; however, the United Nations is pursuing "universal affordable Internet access" as a means for global economic improvement, which will increase Internet access to the third world.[300] If Moore's law holds true for the future, as it has for the last fifty years, computing power will double every two years.[301] These three facts alone suggest that innovation in the field of Internet technologies is going to grow.

Even with the Internet's projected advancements, the future of crime and technology, like other trends, is difficult to precisely predict. John Nasibett, a renowned expert in the field of future studies, has stated, "Trends, like horses, are easier to ride in the direction they are going."[302] This would mean that trends are not only difficult to predict, but easier to manage if they are known. A dynamic environment like the one created by crime and technology make predictability difficult individually, let alone when combined. Despite being difficult to predict, the one trend that appears certain is that

---

[299] Keith Breene, "What Is the Future of the Internet?" World Economic Forum, accessed October 11, 2017, https://www.weforum.org/agenda/2016/01/what-is-the-future-of-the-Internet/.

[300] Tim Sandle, "UN Thinks Internet Access Is a Human Right," *Business Insider*, July 22, 2016, http://www.businessinsider.com/un-says-Internet-access-is-a-human-right-2016-7; "Internet Users," Internet Live Stats, accessed November 10, 2017, http://www.internetlivestats.com/Internet-users/.

[301] Goldstone, Jones, and Roberts, "Group Path Formation," 612.

[302] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Kindle edition (New York: Oxford University Press, 2014), 247.

crime and law enforcement will continue to be shaped, influenced, and evolved by technology.

As technology innovations continue to rapidly advance, so too will possibilities for the advancement of crimes facilitated by those technologies. As new technological innovations are designed, criminal typology will evolve, new categories of crime will emerge, old investigative techniques will become obsolete, and deviant behavior and criminal justice will continue to influence one another. The future holds more opportunities for hybrid crime to mature and change. Border-related crime, and all other crimes, will be facilitated by Internet technologies in the future.

Future research should continue the effort of predicting how technologies will afford crime, working to analyze evolving crime, and distinguishing techniques that can deter hybrid and other categories of crime. It is difficult to conduct research on future unknowns, but perhaps future predictions about the border-related crime of smuggling can be used to help predict which technologies might facilitate crime. According to Peter Andres, "Anything that crosses a national border can be used for smuggling."[303] Of even more importance, he states, "most smuggling parallels the methods and routes of legal commerce."[304] Perhaps the strategic technology trends for business could be used as a guide to predict possible technologies that might be used for crime. If that is the case, according to the Gartner business consulting firm, the current strategic technology trends include "artificial intelligence, intelligent apps and analytics, intelligent things, digital twins, cloud to the edge, conversational platforms, immersive experience, blockchain, event-driven model, and continuous adaptive risk and trust."[305] One or more of these technologies might hold the next affordance to disrupt crime, just as Tor and Bitcoin held the affordances that allowed Ulbricht to create the Silk Road.

Darknet marketplaces are still an issue for future research. Even though the Silk Road, Silk Road 2.0, AlphaBay, Hansa, and many other darknet marketplaces have been

303 Andreas, *Border Games*, 521.

304 Ibid.

305 "Top 10 Strategic Technology Trends for 2018," Gartner, October 3, 2017, www.gartner.com/doc/3811368?srcId=1-7251599992&cm_sp=swg-_-gi-_-dynamic.

seized by law enforcement, others remain active. As of the writing of this thesis, there are at least twelve darknet marketplaces, operating under the names The Majestic Garden, Valhalla, Dream Market, Russian SR, WayAway, Cannabis Growers and Merchants Cooperative, WallStreet Market, Sourcery, ZION, Berlusconi Market, Italian Deep Web, and HYDRA (Russian).[306] Tor is still alive and well and affording anonymity to sustain these darknet marketplaces. While Tor is still an effective anonymizing software, others have emerged, including Tails, I2P, Freenet, Freepto, Subgraph OS, Whonix, Peerblock, Disconnect, and Tox.[307] Future research could include analyzing these technologies and other tools used by darknet marketplaces.

The goal of this thesis was to identify the challenges law enforcement faces when countering the illegal movement of people and goods facilitated by the Internet. While this research has provided several findings and prescriptive recommendations, it is just a small step into a complex topic. Further study is required to determine technologies that may one day afford crime, how affordance theory and other frameworks can uniquely advance criminal justice, and what new tools can help law enforcement battle upcoming challenges. There is a lot more work ahead. This study is just the tip of the iceberg.

306 "DNStats - Online Darknet Market Index and Monitor," accessed October 12, 2017, https://www.bing.com/cr?IG=08AD2659BDEB487CAFC57CFC63EC7FC8&CID=19B85A3059A46B983119512958A26AC8&rd=1&h=_7oRGJjwig7o4_MukCaC2woGtBW0xvkKItp7TZNgWe0&v=1&r=https%3a%2f%2fdnstats.net%2f&p=DevEx,5058.1.

307 Adarsh Verma, "5 Best Alternatives to Tor Browser to Browse Anonymously," *Fossbytes*. November 4, 2017, https://fossbytes.com/best-alternatives-to-tor-browser-to-browse-anonymously/; "Whonix vs Tails • r/TOR" Reddit, accessed November 19, 2017, www.reddit.com/r/TOR/comments/40p3xy/whonix_vs_tails/; "PeerBlock Lets You Control Who Your Computer 'Talks to' on the Internet," Download.com, September 23, 2012, http://download.cnet.com/PeerBlock/3000-10435_4-75328692.html; "Disconnect," accessed November 19, 2017, https://disconnect.me/; "A New Kind of Instant Messaging," Project Tox, accessed November 19, 2017, https://tox.chat/.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alsaedi, Noor, A. Sali Fazirulhisyam Hashim, and Fakhrul Rokhani. "Detecting Sybil Attacks in Clustered Wireless Sensor Networks based on Energy Trust System (ETS)." *Computer Communications* 110 (2017): 75–82.

Andreas, Peter. *Border Games: Policing the U.S.-Mexico Divide*, 2nd edition, Kindle. Ithaca, NY: Cornell University Press, 2009.

———. *Smuggler Nation: How Illicit Trade Made America*, Kindle edition. New York: Oxford University Press, 2013.

Bilton, Nick. *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road*. New York: Portfolio/Penguin, 2017.

Bryant, Robin, and Sarah Bryant. *Policing Digital Crime*. Burlington, VT: Ashgate, 2014.

Darwin, Charles. *The Origin of Species by Means of Natural Selection* (Annotated), Kindle edition. G. Books, 2011.

Décary-Hétu, David, and Luca Giommoni. "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous." *Crime, Law and Social Change* 67, no. 1 (2017): 55–75.

Department of Homeland Security. "FY 2018 Budget in Brief." Accessed December 1, 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf.

Douceur, John R. "The Sybil Attack." Microsoft, accessed November 18, 2017. https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf.

Eggers, William D. *Delivering on Digital: The Innovators and Technologies that Are Transforming Government*, Kindle edition. New York: Rosetta Books, 2016.

Elwell, Craig K., M. Maureen Murphy, and Michael V. Seitzinger. *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, CRS Report No. R43339. Washington, DC: Congressional Research Service, 2015.

Finklea, Kristin M. "The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement." *Journal of Current Issues in Crime, Law and Law Enforcement* 5, no 1/2 (February 2012): 29–67.

Gibson, James J. *The Ecological Approach to Visual Perception*. Boston: Houghton Mifflin, 1979.

Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan, "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes." *Criminology & Public Policy* 16, no. 1 (2017): 99–117.

Goldstone, Robert L., Andy Jones, and Michael E. Roberts. "Group Path Formation." *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 36, no 3 (May 2006): 611–620.

Goodman, Marc. *Future Crimes: Everything is Connected, Everyone Is Vulnerable and What We Can Do about it*, Kindle edition. New York: Anchor Books, 2015.

Graham-Rowe, Duncan. "Sniffing Out Illicit BitTorrent Files." *MIT Technology Review*, October 22, 2012. https://www.technologyreview.com/s/412021/sniffing-out-illicit-bittorrent-files/.

Holt, Thomas J. "Exploring the Intersection of Technology, Crime, and Terror." *Terrorism and Political Violence* 24, no. 2 (March 14, 2012): 338–340.

Huang, Hsin-Yi, Po-Lin Chen, and Yu-Chen Kuo. "Understanding the Facilitators and Inhibitors of Individual's Social Network Site Usage." *Online Information Review* 41, no. 1, (2017): 85–101.

Jarvis, Lee, Stuart MacDonald, and Lella Nouri. "The Cyberterrorism Threat: Findings from a Survey of Researchers." *Studies in Conflict & Terrorism* 37, no. 1, (September 2013): 68–90. doi:10.1080/1057610X.2014.853603.

Jarzabkowski, Paula, and Sarah Kaplan. "Strategy Tools-In-Use: A Framework for Understanding 'Technologies of Rationality' in Practice." *Strategic Management Journal* 36 (March 2014): 537–558.

Lacson, Wesley, and Beata Jones. "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road." *International Journal of Cyber Criminology* 10, no. 1 (January–June 2016): 47–51.

Maras, Marie-Helen. "Inside Darknet: The Takedown of Silk Road." *Criminal Justice Matters* 98, no.1 (December 2014): 22–23. doi:10.1080/09627251.2014.984541.

Marsh, Leslie, and Christian Onof. "Stigmergic Epistemology, Stigmergic Cognition." *Cognitive Systems Research*, 9 (2008): 136–149.

Massey, Douglas S., Jorge Durand, and Karen A. Pren, "Why Border Enforcement Backfired," *American Journal of Sociology* 121, no. 5 (March 2016): 1557–1600.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin. Accessed December 1, 2017. https://bitcoin.org/bitcoin.pdf.

Nieto-Gomez, Rodrigo. “Stigmergy at the Edge: Adversarial Stigmergy in the War on Drugs.” *Cognitive Systems Research* 38 (June 2016): 31–40.

Norman, Don. *The Design of Everyday Things*, rev. edition. New York: Basic Books, 2013.

Pannequin, Remi, and Andre Thomas. “Another Interpretation of Stigmergy for Product-Driven Systems Architecture.” *Journal of Intelligence Manufacturing* 23 (2012): 2587–2599.

Privat, Gilles. “Phenotropic and Stigmergic Webs: The New Reach of Networks.” *Universal Access in the Information Society* 11, no. 3 (2012): 323–335.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.

Robey, Daniel, Chad Anderson, and Benoit Raymond. “Information Technology, Materiality, and Organizational Change: A Professional Odyssey.” *Journal of the Association for Information Systems* 14, no. 7 (July 2013): 386–389.

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Kindle edition. New York: Oxford University Press, 2014.

Syallow, Maureen. “Media Dependency Theory in Use.” Academia.edu, accessed November 18, 2017. http://www.academia.edu/9834996/Media_ Dependency_Theory_in_Use.

TEDxTalks. “Christopher White: Fighting the ‘Dark Web.’” YouTube video, 14:16. From a TedxTalk on the Oklahoma State University campus on April 10, 2015. Posted April 30, 2015. https://www.youtube.com/watch?v=9QsjkJcUznA.

“Tor Security Advisory: ‘Relay early’ Traffic Confirmation Attack.” *Tor Blog*, July 30, 2014. https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack.

Van Buskirk, Joe, Raimondo Bruno, Timothy Dobbins, Courtney Breen, Lucinda Burns, Sunresan Naicker, and Amanda Roxburgh. “The Recovery of Online Drug Markets Following Law Enforcement and other Disruptions.” *Drug and Alcohol Dependence* 173 (2017): 159–162. doi:10.1016/j.drugalcdep.2017.01.004.

Zhang, Wei, Haiyan Zhao, Yi Jiang, and Zhi Jin. “Stigmergy-Based Construction of Internetware Artifacts.” *IEEE Software* 32, no. 1 (January/February 2015): 58–66.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California